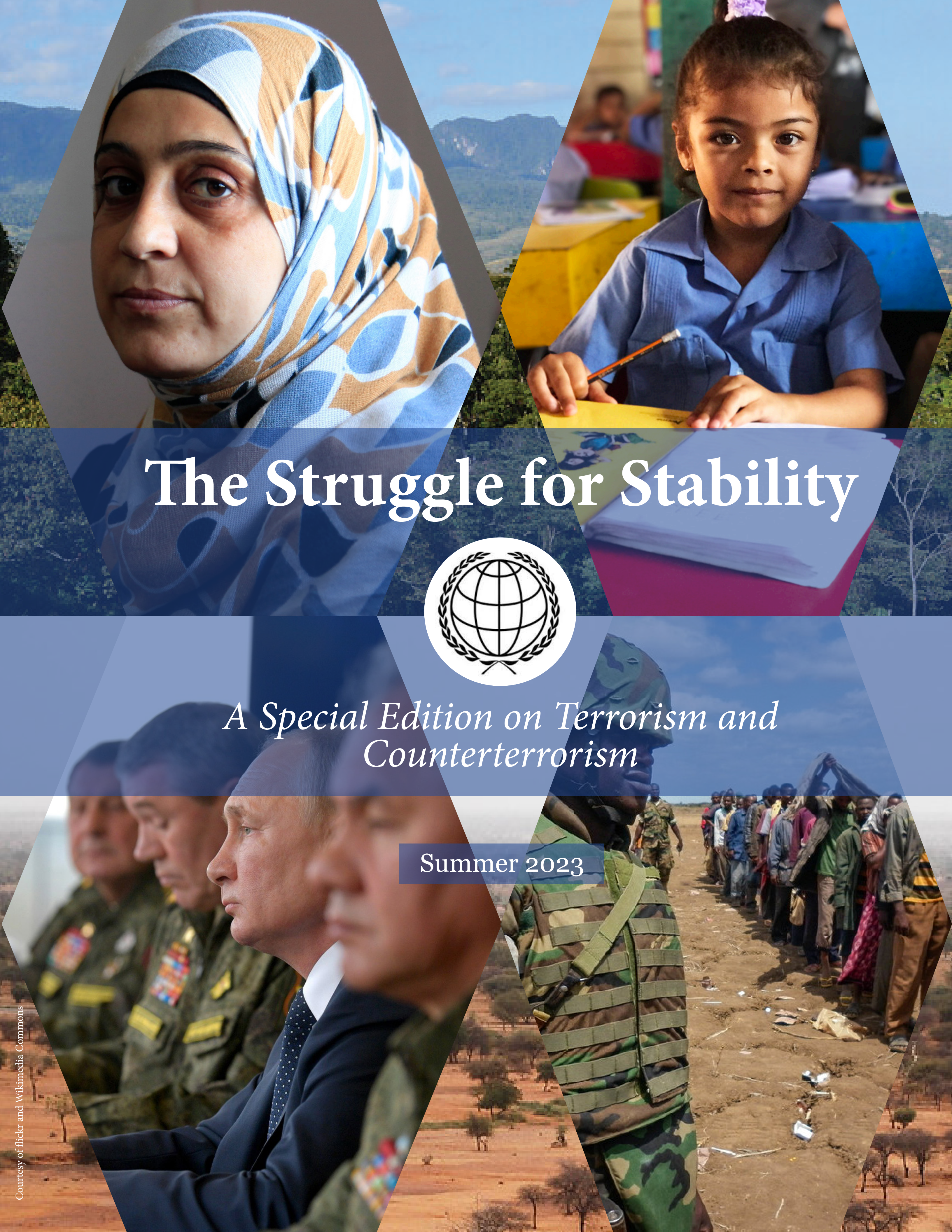
The Struggle for Stability

A Special Edition on Terrorism and Counterterrorism

Summer 2023



Courtesy of flickr and Wikimedia Commons

From the Editor

A Note to the Reader

The Diplomatic Envoy

Dear Reader,

Thank you for taking the time to read The Diplomatic Envoy's 2023 Summer Edition on Terrorism and Counterterrorism.

Terrorism is a force that is ever-present within the international system. Shifting international dynamics and technological advances have led to the evolution of how terrorist acts are enacted and viewed, while presenting new options for the continued global fight against these actions. It is imperative that international actors continue to identify new trends and come together to respond with global action to increase security and stability. In this edition, we aim to bring you in-depth analysis on several facets of what this crisis looks like in 2023. Within this magazine are six stories written by some of our best staff writers that cover various angles of this issue.

On behalf of the Editorial Board, we hope you enjoy reading our 2023 Summer Edition. If you'd like to become a part of our team, please scan the QR code on the back cover of this magazine or reach out to anyone on the Editorial Board. To read more of our work, visit our website, listed on the back cover of this edition.

Hazard Zet Forward!

Andrea Hebel
Editor-in-Chief

SCHOOL OF DIPLOMACY AND INTERNATIONAL RELATIONS
SETON HALL UNIVERSITY

This publication is made possible through the generosity of the Constance J. Milstein, Esq., Endowed Fund.

The views expressed in *The Diplomatic Envoy* are those of the writers and are not intended to represent the views of the School of Diplomacy, Seton Hall University, or the CJM Fund.

For more information on sources, go to blogs.shu.edu/thediplomaticenvoy

CONTRIBUTORS

Ashley Skladany

Joseph Brennan

Kiara McGaughey

Madeline Field

Pranali Jain

Sophie Ulm

TABLE OF CONTENTS

The Robust Roles of Women in Terrorism Cannot Be Overlooked

Madeline Field | Staff Writer

Courtesy of the World Bank Photo Collection(flickr)

When you think of terrorists, do you ever think of women?

When women are portrayed as terrorists, stereotypes abound; they are “schoolgirls,” “mothers, monsters, whores,” and “shy housewives.” They are women manipulated by their husbands to commit violence. They are caregivers who betray their children by leaving them behind. Women are (often accurately) perceived as victims of terrorist oppression rather than architects of terrorist violence. The idea of female terrorists offends gendered conceptions about the stereotypically passive roles women take in society, especially in conflict.

Yet the reality of female terrorism complicates those narratives. Many women are eager and active members of terrorist groups and participate in terrorism at higher rates than is assumed. Thus, studying women in terrorism is essential to further gendered perspectives on counterterrorism. To tackle the most critical counterterrorism challenges of our time- the rise of Islamic terrorism in the Sahel, the prospect of repatriating former ISIS devotees, and the flourishing of right-wing terrorism- gender-conscious approaches to counterterrorism are necessary.

What role do women play in terrorist organizations?

Women have played active roles in terrorist groups dating back to the late-1800s, with Russians like Vera Zasulich and Sofia Perovskaia directing assassination attempts as early as 1878. Women have been identified as terrorists throughout history in various politically and economically unique countries, from Chechnya and Colombia, to Indonesia and Iraq, to the UK and the U.S.

Women began to gain widespread prominence as terrorists in the 60s, 70s, and 80s amidst a radical feminist wave. At that time, terrorist groups such as West German Rote Zora and the May 19th Communist Organization, the first and only exclusively female terrorist group in existence that notably bombed the U.S. Capitol, dominated headlines. Women rose to prominent and high-ranking positions in left-wing organizations, which typically sought to overthrow capitalist governments due to embracing more egalitarian, gender-equitable ideologies.

Sharply usurping the prominence of leftist terrorism has been right-wing domestic terrorism and Islamic terrorism. While until recently, women have typically been shut out of right-wing organizations due to leaders’ ideologies, scores of women have gained strategic prominence in Islamic terrorist organizations. In fact, of the living foreign fighters who have fled to ISIS-controlled territory, roughly 13 percent are women.

The idea of female terrorists offends gendered conceptions about the stereotypically passive roles women take in society

The ideological variety of terrorist groups frequented by women is only usurped by the vast array of roles they play in said organizations. Undoubtedly, in jihadist and radical far-right groups, women are increasingly recruited to play active roles in terrorist groups due to their strategic value.

Women make great evangelizers. Women are traditionally viewed as more trustworthy and have higher-network activity than males, making their advice more plausible to many other females. Thus, they can attract more women and even men to join their cause and help expand an organization’s domestic and overseas footprint.

Women also elicit sympathy for terrorist groups and may normalize violence. As recently as the 1960s, for example, white women and their subsequent interactions with black males were utilized as symbols by the Ku Klux Klan to condone racism, lynchings, and other extra-judicial killings and garner sympathy for the white cause. Women who join terrorist groups may be viewed more sympathetically than men by local communities and garner more attention for their attacks, furthering the organization’s goals and entrenching violence in society,

Women also make effective combatants. In many societies, especially those in which traditional Islamic gender roles dominate, women and children can evade the many strict security protocols designed to foil male terrorists. In many countries, women and children are considered sacred and unlikely combatants, meaning targets may let their guard down in their presence. These vulnerabilities may make them more effective purveyors of violence than men.

While women have played active combat roles in radical communist terrorist groups such as FARC, proving to be fierce guerrilla fighters, women more recently seem to be utilized most frequently as suicide bombers. Female suicide bombings have occurred across many countries, such as Chechnya, Palestine, Uzbekistan, Iraq, Lebanon, Indonesia, and Morocco, and many organizations have outstripped male suicide bombings. The Nigerian terrorist group Boko Haram, for example, utilized nearly 500 women in suicide bombings in less than four years, causing over 4000 casualties. Suicide bombings enacted by females are four times as deadly as males due to less rigorous security screenings for women.

Women also function in non-combat roles as money launderers, homemakers, and sex slaves. In the Syrian refugee camp Al-Hawl, former ISIS wives have evaded police detection, allowing them to proselytize and keep the caliphate alive through inconspicuous activities such as money laundering. This marks a significant break from female activities at the height of the caliphate; in those years, female recruits were immediately married to jihadis to have children shortly thereafter. Having “ISIS children,” much like money laundering, was deemed ideologically essential to reproducing the caliphate and a fitting role for women to adopt. This "homemaker" phenomenon is also seen in Boko Haram and Al Shabab, although the latter gives fighter wives much more autonomy and allows them to adopt more significant organizational roles.

While women tend not to head up terrorist groups, their utility in creating terror and unmistakable role in continuing the growth of terrorist organizations make them an essential part of counterterrorism strategy. With the rise of terrorism in the Sahel and Southeast Asia, the question of how women will be used is important. So far, they have primarily served in supportive roles as cooks, wives, and suicide bombers, but those roles may change.

Why do women join?

Not all women affiliated with terrorist organizations are drawn to bloodlust or radical ideology. Some women are coerced into joining or directly kidnapped by militant groups, then forced to commit suicide bombings or placed into de facto sex slavery. Nevertheless, although it is unclear what percentage, many women join through their own free will. It is undoubtedly vital to understand female motivations for joining terrorist organizations.

Understanding motivations can, however, be complex. Decades-long attempts at teasing out even a typical (i.e., male) "terrorist profile" have largely failed. Domestically, according to Brookings, evidence suggests that the "frustrated expectations of individuals for economic improvement and social mobility" or "relative deprivation" of well-educated yet under-employed individuals within a population may push the adoption of radical social theories like terrorism to express political frustration. People who join terrorist groups tend to be younger and more susceptible to recruitment that promises them belonging and purpose. Yet relying exclusively on age, race, ideology, and socioeconomics fails to predict susceptibility to terrorist behavior.

Unsurprisingly, profiles of female terrorists are even less understood and assumed to be anomalous. A nominal number of studies on female terrorists are published, and even fewer examine non-jihadi women. In a rare background study by NC State University of 250 women and men involved in jihad, researchers found a mere two percent of jihadi women had criminal records. Women tended to be younger than their male counterparts and were also three times as likely to be unemployed as men.

Motivations, however, are what drive susceptible women to join. Lea-Grace Salcedo of the Marshall Center succinctly delineates between push and pull factors for female involvement. Pull factors for women are desires "for a new environment, pride, support of a political cause, free education and training, image, and access to social and political roles," and push factors are "deprivation, redemption and honor, revenge, romantic ties, family influence, commitment to an ideological cause, traumatic experiences, and protection of self and family." Concretely, motivations may be desires to express female agency, be tied to personal grievances, and be influenced by propaganda which promises another entirely different experience.

The Australian Institute of International Affairs writes that many women may view "extremist ideology as 'freeing' and a choice of their own, despite the draconian way they are often treated in extremist groups." As in the case of ISIS' brutal all-female Al-Khansaa brigade, a feared morality police division of ISIS, some women may defer to traditional values and view joining a terrorist group as a sort of rebellion against loose morality. Another researcher characterizes voluntary female recruitment in Al Shabab as a sense of meaning, "a struggle to exercise agency within systems of oppression in patriarchal setups with the lure for emancipation within the Al-Shabaab network and the utopian caliphate." To the casual observer, it seems complicated to imagine that women would gain a sense of empowerment from terrorist groups- modern terror groups like Al Qaeda or far-right movements tend to marginalize women- but regardless, many do.

Like with men, personal grievances may also drive recruitment. This was the case for many members of the Black Widows, a prominent anti-Russian Muslim group that utilized female suicide bombers in high-publicity attacks and is infamous for a five-day hostage crisis in a Russian theater that killed nearly 200 people in 2002. In the case of the Chechen Black Widows, desires for political autonomy were coupled with grief and cultural norms of revenge; many women described being motivated by the deaths of their husbands and fathers during the First and Second Chechen Wars.

For others, especially Western women, clever propaganda targeting sympathetic women can prove incredibly influential. Reports in 2015 of women as young as 15 convinced to join ISIS online by propagandists who sold visions of romance and utopian politics were shocking. These girls were deeply influenced by viral depictions of shelled Syrian cities and crying orphaned infants, who saw their joining as a twisted way to save Muslims. Such recruitment tactics are also seen in QAnon propaganda, which weaponized a hashtag, #savethechildren, and allegations of an underground child sex trafficking ring run by prominent liberal government officials, to draw American mothers into the organization.

> *Unsurprisingly, profiles of female terrorists are even less understood and assumed to be anomalous.*

Motivations for joining terror groups vary, with some attractions similar to male motivations. With most current research focusing solely on foreign women joining international terrorist groups, identifying a proclivity to join a terrorist group based on ideology or behavior alone is even more difficult.

How is the issue of women terrorists depicted?

Media often sensationalizes cases of women who join terrorist organizations or commit terrorist acts, complicating counterterrorism efforts. Research indicates that reports of young women being lured to ISIS through social media "emphasized their gender and portrayed their actions as deviant from appropriate performances of femininity," as women are typically represented as victims of violence, not perpetrators of terrorism. Since the concept was so shocking and rare to the everyday reader, depictions of such women have enormous staying power in how they are perceived by the public, making them particularly susceptible to stereotyping.

According to researcher Brigitte L. Nacos, such misinformed framings include commentaries on physical appearance and allegories to gender extremism, insinuations that motivations are due to family or "for the sake of love," manufactured comparisons between them and males (because no "real" woman would be a terrorist), and suggestions that such women are "bored, naïve, out-of-touch-with-reality." A salient example of these framings is the case of the 'ISIS schoolgirls', three teenagers who abruptly left their lives in a middle-class London neighborhood and traveled to Syria, and the female 'Black Widows' of Chechnya.

Women terrorists have used these framings to their advantage. In the aftermath of the January 6th insurrection, lawyers for women arrested have drawn "attention to their clients' responsibility for care work (including their roles as mothers and wives) and their compassion" to make the case for more lenient sentencing, according to NBC News. When comparing sentencing lengths, these rhetorical appeals have largely been successful.

Evidently, such framings affect women in many spaces but are particularly noxious in the given context. According to political scientists and reported in The Security Distillery, depictions of female inclusion in political violence as 'unnatural' negate female agency and deemphasize 'legitimate' reasons for joining terrorist groups. Incorrect framings may be dangerous in that they distort conceptions of why women join terrorist organizations, complicating preventative measures for women who may have been radicalized. Inaccurate depictions of female terrorists may also be problematic because they tend to prove more elusive to the public, confounding detection and making it more challenging to foil their plots.

Just as they can recruit, women can play an active role in mitigating terrorism and utilize their social networks to discourage radicalization.

What does all this mean?

Research efforts must account for gendered perspectives to understand the role of women in terrorism. Women play numerous roles in terrorist organizations, from financers and human traffickers to recruiters and guerrilla fighters. Still, many in the general public are unaware of the lengthy history of female terrorism or non-traditional methods of terrorist involvement.

There is also a perceived lack of research on female terrorism because much of it goes unpublished and is generally not integrated into the terrorism body of research. Undoubtedly, women play roles in terrorist organizations beyond 'housewife' and 'suicide bomber.' Yet information on women as money launderers, human traffickers, and financers is scarce. Although major studies of male terrorists have proved elusive, larger-scale studies of female terrorists could help researchers understand female motivations, especially those of women in the Sahel.

Just as they can recruit, women can play an active role in mitigating terrorism and utilize their social networks to discourage radicalization. Women are often trusted members of the community, and their discouragement of terrorism has the power to influence younger boys, girls, and adults.

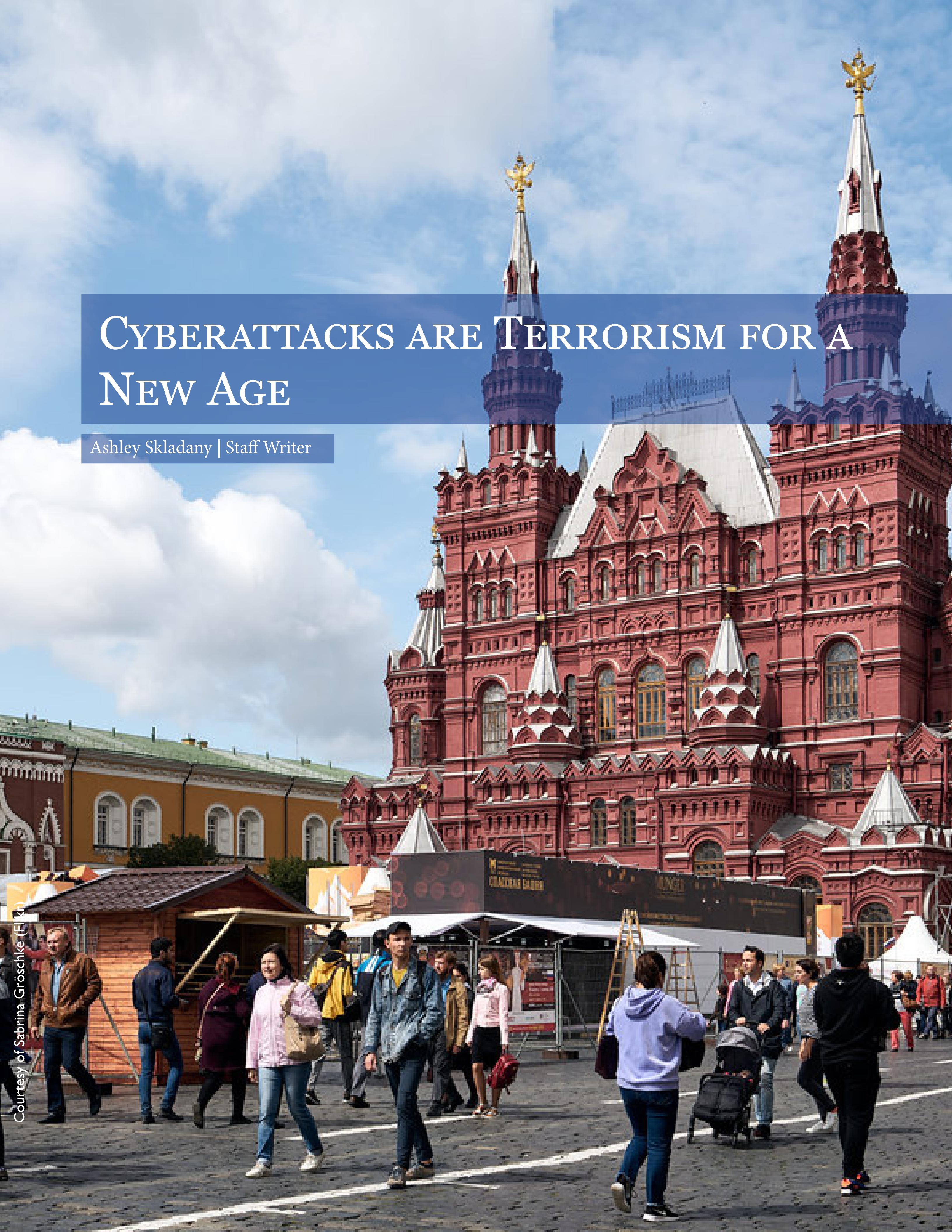
Unfortunately, most counterterrorism efforts fail to account for the gendered perspectives of women or dismiss female terrorists altogether. In 2021, the Biden Administration made strides towards addressing female agencies in terrorism, establishing the Gender Policy Council and the role of National Intelligence Officer for Gender Equality, who will presumably "coordinate intelligence support for the Council's work on issues implicating national security." However, in just the short description provided by the Council, it appears it is more focused on women as victims of violence rather than perpetrators. An apparent hesitancy to see women as agents of terrorism leaves communities susceptible to further radicalization by ignoring the reasons that may push women to join terrorist groups.

As terrorism proliferates in Africa, countries deal in the Middle East with the repatriation of former extremists, and right-wing domestic terrorism grows, it is more important than ever to have a non-biased, well-rounded perspective towards women and terror.

Contact Madeline at madeline.field@student.shu.edu

Cyberattacks are Terrorism for a New Age

Ashley Skladany | Staff Writer



Courtesy of Sabrina Gröschke (Flickr)

In May of 2021, U.S. citizens were left in disarray as gasoline supplies to the Eastern part of the country were cut by 45 percent, forcing cars to line up for blocks to fill their tanks. The direct cause was cited as a "cyberattack" on the Colonial Pipeline, which carried gas and other fuels from Texas to the East Coast, according to Maryville University. In June of the same year, meat suppliers faced their own unique cyberattack on factories owned by JBS, a company that supplies more than one-fifth of the beef consumed in the United States. These two instances did not only financially impact gasoline and meat suppliers, but extended their reach to affect millions of individuals. Yet, the frequency of these kinds of damaging attacks is only increasing. According to a Congressional Research Service report, researchers discovered that for victims across 24 countries, cybercrime incurs an annual cost of $388 billion.

By 2030, insurance firm Marsh McLennan predicts 30 billion technological devices will be in use. For cyber terrorists, this creates a wider range of vulnerable governmental and organizational assets susceptible to attack and exploitation. In order to protect individuals, governments must try to decipher a way to successfully tackle this billionaire-dollar enterprise. However, the unique nature of the digital sphere allows for covert operations and swift information warfare to be easily weaponized by terrorists, which creates unprecedented and difficult challenges for governments to understand, starkly setting cyberterrorism apart from traditional acts of terrorism.

> *... the unique nature of the digital sphere allows for covert operations and swift warfare to be easily weaponized by terrorists...*

An out of service gas pump in Virginia after a cyber attack on the Colonial Pipeline. Courtesy of Famartin(Wikimedia Commons)

Cyberterrorism is a relatively new frontier. Conversations surrounding the topic did not begin until the late-1990s. In the United States, the bombing of the World Trade Center in 1993 as well as the Oklahoma bombing in 1995 are typically cited as the first high-profile attacks that consequently propelled the U.S. Department of Defense to conduct its first warfare exercise to measure the cybersecurity of its systems. It was not until the 9/11 attacks, however, that serious legislative measures, such as the Patriot Act of 2001 and the Terrorism Risk Insurance Act of 2002, were introduced in attempts to tackle cyber terrorism. But as of today, the laws passed have yielded limited success.

The New York Times writes that the FBI considers "ransomware as grave a danger to U.S. interests as terrorism in the aftermath of the attacks of September 11, 2001." In other words, proper solutions need to be enacted against this ever-evolving threat. Nevertheless, understanding what exactly "cyber terrorism" entails can be difficult. Dataconomy, a popular technology news site, describes cyber terrorism as "the use of computer networks or systems to intentionally cause damage, disrupt operations, and/or intimidate individuals," a definition that commonly aligns with other sources. This includes disrupting the internet's technological foundation, government computer networks, or critical civilian systems, such as financial networks or mass media. The actors, ranging from nonstate, state, and private, "may have a variety of goals," Dataconomy shares, attempting to create chaos or intimidation for financial, political, or social gains. The Congressional Research Service, however, highlights that the digital realm is ever-expanding. The complexity of the cyber sphere and its nature means that there is no clear and concise definition when it comes to outlining cyber terrorism. Because distinctive boundaries are lacking, so is a proper, widely understood, and accepted definition. Thus, grappling with cyberattacks can be a complex phenomenon for both companies and governments.

The 2017 WannaCry and NotPetya incidents mark two of the most significant global cyber-terrorist attacks that exemplify the alarming rate at which the methods and consequences of cyberterrorism can escalate. The Guardian explains that these attacks in the UK shut down computers in over 80 National Health Service facilities, resulting in thousands of canceled appointments and overwhelmed hospital systems. The attack was born from two newer innovations: encryption and Bitcoin. Bitcoin has offered a new outlet for terrorists, suddenly allowing ransomware creators to take payment without the hassle of the conventional banking system. Encrypted files have resulted in the creation of ransomware, a software that holds people's information hostage until they pay a requested sum.

WannaCry was the first ransomware attack that the world watched disrupt society on such a massive scale, with its impacts affecting organizations in over 150 countries and leading to losses of more than $300 million, Marsh McLennan reports. The attack had severe implications and life-threatening consequences, hindering the ability of the NHS to provide proper care for its patients in the UK. However, the head of the National Audit Office (NAO), Amyas Morse, said that WannaCry "was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practice." This raises a paramount concern regarding how exactly the attack managed to take out a significant portion of the NHS in just a matter of days. Fixes for the vulnerabilities that were exploited had already been released in March, the NAO report states. However, these fixes were not implemented, leading to a careless mistake that had disastrous ramifications. The outcome of the WannaCry incident exemplifies the necessity for enhanced and mandated digital awareness training within organizations.

Only a month later, another attack dubbed NotPetya occurred, which built on the lessons of WannaCry by using the same weaknesses to spread within the corporate network. The ransomware was distributed to victims via a hacked version of a major accounting program used in Ukraine. The program had extensive internal networks, enabling the threat to travel far outside of Ukraine's borders and cause chaos. However, the attacks were not suspected to be monetarily motivated as WannaCry was. The Guardian explains that the ransomware was improperly coded, meaning that even if users did pay up, their data could never be retrieved. The evident lack of concern regarding the collection of money by the ransomware authors establishes that profit was not the goal of this attack. The NATO Cooperative Cyber Defense Centre of Excellence agrees that "malware analysis supports the theory that the main purpose of the malware was to be destructive because the key used for encrypting the hard disk was discarded."

The realization that NotPetya was most likely conducted for the purpose of destruction heeds further concerns surrounding the ransomware's target of a Ukrainian accounting program. The Guardian emphasizes that "[t]he country has long been at the forefront of cyberwarfare, constantly trading digital blows with its neighbor Russia even while the two countries trade actual blows over Crimea." Taking into account the nature of the NotPetya ransomware, it is very possible that the global outbreak was a demonstration of power, "probably launched by a state actor or non-state actor with support or approval from a state." The National Cyber Security Centre of the United Kingdom asserts that "the Russian military was almost certainly responsible for the 'NotPetya' cyber attack." Though not conclusively verified, it is a reasonable analysis, as it would not be the first time in which Russia engaged in state-backed cyber-attacks categorized as cyber terrorism. For example, in 1996, Russia led a two-year campaign classified as an advanced persistent threat (APT). Through the theft of massive amounts of classified information from numerous government agencies, U.S. national security and strategies were left vulnerable and exposed.

The Russia-Ukraine war offers greater insight and analysis into the way cyberspace is being utilized for state-backed cyberterrorism, as well as defense. According to the German Institute for International and Security Affairs (SWP), "In August 2022, the Computer Emergency Response Team of Ukraine reported over 1,123 cyberattacks in the first half of the war." At the beginning of the war, more specifically, "Moscow launched what may have been the world's largest ever salvo of destructive cyber-attacks against dozens of Ukrainian networks," The Carnegie Endowment writes. Russia's attack resulted in the disruption of the Viasat satellite communications network, occurring

Russia has launced cyberattacks on Ukrainian networks, slowing military communications. Courtesy of the public domain(rawpixel)

just before tanks crossed the border. With technology becoming ever more necessary for military communications, the result ultimately caused serious delays and the hindrance of Ukraine's initial defense of Kyiv.

Despite this being true, there appears to be a general consensus that Russian cyber operations during the war have not been as impactful or eventful as originally expected. "Russia's main cyber activity in Ukraine has probably been intelligence collection," Nick Beecroft, Carnegie Endowment Scholar, shares. "Russian hackers have most likely sought to gather [high-value] data" that can later be leveraged effectively. Information collection can give rise to substantial threats, which could intensify the conflict considerably. For instance, acquiring real-time geolocation data has the potential to enable actions like the assassination of Ukrainian President Volodymyr Zelenskyy, or the precise and timely targeting of Ukrainian troops, Carnegie Endowment Scholar, Jon Bateman, emphasizes. The usage of Russian hackers as a part of the war effort is the result of Russia's support of state-backed cyber terrorism. BAE Systems, an international aerospace security company, describes such hackers as being given a "license to hack." In other words, they may have permission to conduct destructive digital attacks, without fear of legality, with both support and resources from the government.

The New York Times writes that the FBI considers "ransomware as grave a danger to U.S. interests as terrorism in the aftermath of the attacks of September 11, 2001."

These individuals or groups of hackers are employed with the intent to compromise and destabilize the enemy's digital infrastructure under the aims of the government. This is done through various methods of digital terrorism, most commonly those including ransomware, DDoS attacks, or data breaches. Though such actions can also technically be classified as cyber warfare, both cyber terrorism and warfare are united through their common destructive goals. Moreover, cyber-terrorism tactics, such as hiring hackers, are employed as tools as a part of a state's war efforts in the digital sphere, meaning that cyberterrorism can be seen as a key yet distinctive component of cyber warfare.

The heightened attention surrounding the Russia-Ukraine conflict has enabled Ukraine to protect itself against Russian cyber-attacks, thereby mitigating the impacts. Beecroft cites that Ukraine has been able to "deploy cyber defenses at a scale and depth never seen before." The cause, he continues, is "an alliance of competing companies and governments with varying agendas collaborating and learning together to thwart Russian cyber attacks, driven by a shared sense

of outrage at the invasion." The war has demonstrated that cyber defenses can indeed, be successful, granted there is a united front. Researchers at Talking About Terrorism outlined policies needed to tackle cyberterrorism, labeling "the cooperation among states" as "critical." The researchers further argued that there is an overall lack of consensus aimed at creating a proper, coordinated deterrence strategy. As a result, efforts to successfully tackle cyber-terrorism suffer without united accountability from both state and non-state actors.

Forbes defends this point, explaining there is a need for "all countries to utilize the internet for economic, political, and demographic benefit while refraining from activities that could cause unnecessary suffering and destruction," a concept termed as geo-cyber stability. The unparalleled surge of cyber support from the world's most capable companies and governments has unveiled the critical role of the private sector and other government entities in effectively defending digital networks at a national scale. The heightened protection of Ukraine's networks emphasizes how cooperation is critical when defending society from cyber threats. Simply put, a united front of geo-stability employed by states and backed by other important non-state actors as successfully displayed in Ukraine is a must when considering future legislation to tackle cyber terrorism.

Cyber-terrorism only continues to pose itself as a dangerous threat as more sophisticated technologies continue to develop. Many countries' national security will remain at risk unless governments around the world can work together to implement greater stability and protection against threats in the digital realm. The lack of an international, digital legal framework is holding the global community back. Without it, there can be no geo-cyber stability and not even a clear consensus as to what cyber terrorism may properly entail.

*Contact Ashley at ashley.skladany@student.shu.edu*ness

The Ongoing Gang Wars in Central America

Joseph Brennan | Associate Editor

Courtesy of Carlosmanuel232(Wikimedia Commons)

Gang activity has dire consequences for nations, leading to social and economic breakdowns.
Courtesy of Walking the Tracks(Wikimedia Commons)

Central America has gained notoriety for its exceptionally high levels of gang violence, particularly in countries like El Salvador, Honduras, and Guatemala. Gangs have evolved into formidable criminal organizations, exerting control over specific territories and engaging in a wide range of illicit activities, which pose significant threats to the region's stability and security. The two most prominent and influential gangs operating in Central America are Mara Salvatrucha (MS-13) and Barrio 18 (Mara 18). Both gangs originated in the United States and later expanded their operations to Central American countries. These gangs are increasingly growing in size and power and are becoming major players in the region's criminal landscape.

MS-13 has a reputation for extreme violence and has expanded its presence beyond Central America, reaching North America and even parts of Europe. Originally formed by Salvadoran immigrants in Los Angeles in the 1980s, MS-13 later established roots in El Salvador, Honduras, Guatemala, and other countries. MS-13 members are identifiable by their distinctive tattoos and hand signs. They engage in a wide range of criminal activities, including drug trafficking, extortion, human smuggling, and contract killings. Their operations often involve intricate networks that span national borders, making it difficult for law enforcement agencies to combat their influence effectively.

Barrio 18 is another significant gang operating in Central America. Much like MS-13, Barrio 18 was originally formed in Los Angeles before expanding operations to El Salvador, Honduras, and Guatemala, where it established a strong presence. Barrio 18 also engages in various criminal activities, including drug trafficking, extortion, robbery, and murder. The gang's influence is characterized by a territorial structure, where different factions control specific neighborhoods or "barrios." This territorial control creates a volatile environment as clashes between rival factions or attempts to expand territories often result in heightened violence and retaliatory acts.

These gangs are increasingly growing in size and power and are becoming major players in the region's criminal landscape.

The activities of these gangs have far-reaching consequences. Drug trafficking and the resulting drug trade, for example, fuel addiction, leading to devastating social and public health consequences. Extortion practices target businesses and individuals, hindering economic growth and creating an environment of fear and instability. Robberies and acts of violence committed by gang members further erode trust within communities and perpetuate cycles of violence. The influence of these gangs extends beyond their direct criminal activities. They often control informal economies within their territories, exerting control over local markets and exploiting vulnerable populations. Moreover, their presence disrupts social structures, leading to a breakdown in community cohesion and a loss of faith in public institutions.

Addressing the issue of gang violence in Central America requires a multi-faceted approach that encompasses law enforcement efforts, community engagement, and social development programs. The complex nature of these criminal organizations demands coordinated regional strategies, intelligence-sharing, and collaboration between law enforcement agencies across national borders. Addressing the root causes of gang involvement, such as poverty, lack of education, and limited economic and social opportunities, is crucial for breaking the cycle of violence and providing alternative pathways for at-risk youth. Central American governments, with the support of international organizations and partners, continue to work towards dismantling these gangs and mitigating their impact on society. However, it remains an ongoing challenge that necessitates long-term commitment and comprehensive solutions to ensure the safety and well-being of communities in Central America and beyond.

Understanding the root causes of gang violence in Central America is essential for formulating effective strategies to combat this issue. The region's complex socio-economic and historical factors contribute to gang culture and recruitment, particularly among marginalized youth. Socio-economic disparities play a significant role in the prevalence of gang violence. Central America faces significant income inequality, with a small portion of the population controlling a majority of the wealth, while many live in poverty. Specifically in El Salvador, World Food Programme reports that 40 percent of the population has lived in poverty since 2020. This disparity leads to a lack of resources and opportunities for disadvantaged communities, making them more susceptible to gang recruitment. Limited access to quality education, healthcare, and basic services further exacerbates these challenges, leaving young people with few avenues for upward mobility.

Inadequate educational opportunities contribute to the vulnerability of youth to gang recruitment. A deficient education system, marked by underfunding, overcrowded classrooms, and a lack of qualified teachers, hampers academic achievement and confines the potential of young students, often becoming suitable gang prospects. Without access to quality education, young individuals are more likely to turn to gangs as an alternative source of identity, protection, and economic opportunity. Healthcare deficiencies also contribute to gang violence. Limited access to healthcare services, including mental health support, can leave individuals feeling neglected and marginalized. Mental health issues, trauma, and unresolved conflicts within families and communities can drive young people toward gang membership as a means of finding belonging or as an outlet for their frustrations.

Addressing the issue of gang violence in Central America requires a multi-faceted approach that encompasses law enforcement efforts, community engagement, and social development programs.

A scarcity of employment opportunities is another critical factor driving gang violence. High unemployment rates, particularly among youth, create a sense of hopelessness and frustration. The lack of legitimate job prospects pushes young individuals towards illicit activities as a means of survival or to gain financial stability. Family dysfunction and broken social structures also contribute to the vulnerability of youth to gang recruitment. Many families in Central America face challenges such as domestic violence, substance abuse, and parental neglect. These factors can lead to a breakdown in familial support and guidance, leaving young individuals susceptible to the influence of gangs that offer a sense of belonging and identity. Furthermore, the region's history of civil wars and political instability has left lasting scars. These conflicts have displaced communities and eroded trust in public institutions. The aftermath of these wars often includes weak governance, corruption, and inadequate law enforcement, allowing gangs to flourish in environments marked by impunity and limited accountability.

Children read in a classroom in Honduras. Courtesy of Global Partnership for Education (Flickr)

Gangs in Central America establish their dominance through fear and coercion, often resorting to extortion as a means of control. Local businesses and residents are subjected to forced payments known as "war taxes" or "protection fees," which drain resources from already struggling economies. This economic burden hinders development and discourages entrepreneurship, as business owners are hesitant to invest and expand in an environment plagued by violence and intimidation. The climate of fear perpetuated by gangs significantly impedes economic growth and stability. Entrepreneurs, fearing forced closure, may opt to shut down their businesses rather than endure the constant threats and extortion demands. The resulting loss of livelihoods and income opportunities further exacerbates poverty and social inequality within affected communities. In turn, the lack of economic growth and prosperity reinforces the conditions that fuel gang violence, perpetuating a vicious cycle.

Governments in Central America have acknowledged the urgent need to address this problem. One key approach is the strengthening of law enforcement operations. Governments have increased police presences and implemented targeted operations to dismantle gang structures and disrupt their criminal activities. These efforts often involve intelligence-led investigations, arrests, and prosecutions of gang members. By prioritizing public safety and cracking down on gang-related offenses, governments aim to create an environment that is less conducive to gang activities.

Regional collaboration is also crucial in addressing the transnational nature of gang activity. Initiatives such as the Central American Integrated System for the Prevention, Investigation, and Prosecution of Gang Crimes (CIS-GANG) promote information sharing and joint operations between countries. This collaboration strengthens the collective efforts of Central American nations in combating gang activities, enhancing intelligence sharing, and facilitating the extradition of gang members across borders.

Gangs have proven to be adaptable and resilient, often evolving their tactics and strategies in response to law enforcement efforts.

Despite the concerted efforts made by governments in Central America to combat gang activity, however, reducing gang violence in the region continues to be a challenge. Gangs have demonstrated resilience and adaptability, often outmaneuvering law enforcement strategies and exploiting vulnerabilities within the justice system. Corruption within law enforcement agencies poses a significant obstacle to effective anti-gang measures. Some members of the police force, judiciary, or other government institutions may be complicit in or influenced by gang activities. This corruption undermines the trust and legitimacy of law enforcement efforts, allowing gangs to operate with relative impunity. It also hampers successful prosecutions, as corruption within legal systems can manifest in witness intimidation and evidence tampering.

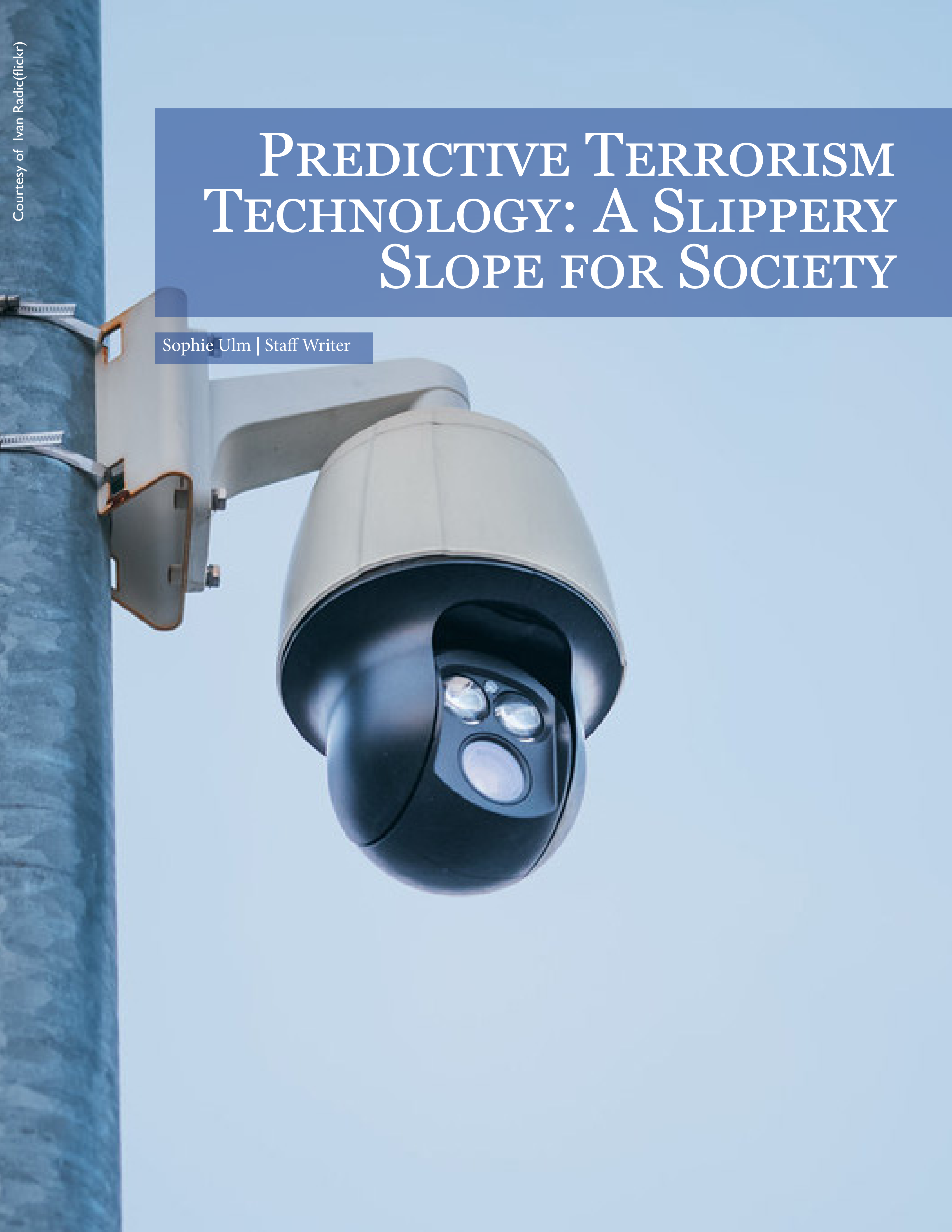
While governments have demonstrated commitment to combating gang violence, numerous challenges persist. Gangs have proven to be adaptable and resilient, often evolving their tactics and strategies in response to law enforcement efforts. On top of corruption within law enforcement agencies, limited resources, including funding and training, impede the implementation of effective anti-gang measures.

Insufficient staffing, outdated equipment, and inadequate training for law enforcement agencies hinder their ability to tackle the complex and evolving nature of gang violence. Additionally, a lack of investment in intelligence gathering, technology, and information-sharing mechanisms can restrict the coordination and effectiveness of cross-border efforts to combat transnational gang networks. Overcrowded prisons throughout the region are filled beyond capacity and lack proper security measures, allowing gang members to strengthen their networks, recruit new members, and plan criminal activities within the confines of the prison walls. In some instances, prisons become de facto headquarters for gangs, further perpetuating their influence and power. Addressing prison overcrowding and implementing comprehensive rehabilitation and reintegration programs are essential in disrupting gang dynamics and preventing their continued expansion.

Addressing social factors involves investing in community development programs, promoting social cohesion, and providing support systems for at-risk youth. By focusing on education, vocational training, and mentorship programs, governments can provide alternatives to gang membership and equip individuals with the skills and opportunities necessary for a productive and lawful life. Economic strategies include job creation initiatives, promoting entrepreneurship, and facilitating access to financial services in underserved areas. By tackling the underlying economic inequalities and creating pathways to economic stability, governments can mitigate the allure of illicit activities and provide individuals with legitimate means of income and advancement.

Political reforms are also crucial in addressing the root causes of gang violence. Strengthening governance, enhancing transparency, and combating corruption are essential for creating an environment where the rule of law prevails. Effective and accountable institutions can restore public trust, ensuring that justice is served and providing a deterrent against gang activities. Addressing the root causes of gang violence requires collaboration between governments, civil society organizations, and international partners. Coordinated efforts and shared best practices can foster innovative approaches to prevention, intervention, and rehabilitation. Regional cooperation, information-sharing, and joint operations are instrumental in disrupting transnational gang networks and tackling the cross-border nature of gang activities.

Contact Joseph at joseph.brennan@student.shu.edu



Courtesy of Ivan Radic(flickr)

Predictive Terrorism Technology: A Slippery Slope for Society

Sophie Ulm | Staff Writer

The use of predictive technology in counter terrorism has emerged as a preventative measure to avoid actions before they occur. These developments come with the ambition of creating a safer environment for people to live in and reducing threats of violent extremist actions. Yet while many have heralded the use of such technology as a means for further protecting the safety of individuals, it also presents an evident threat to individual privacy and freedom which can be seen across the world.

Humanity's desire for safety and protection is strong, as demonstrated by the increasing nature of predictive technology. But many individuals have not yet begun to grapple with the potential negative effects of these measures, which have already been seen in several instances. In China, there has been an increase in predictive technology as a means to continue the oppression of the Uyghur population and other groups seen as societal outsiders. In France, artificial intelligence and predictive technology have been used in a way that creates conflicting requirements for individuals suspected to be threats, leaving them with no way to meet the standards set to lift their restrictions. In the United States, predictive artificial intelligence has been known to solidify racial biases, rather than working to fix them.

[Predictive technology] also presents an evident threat to individual privacy and freedom which can be seen across the world.

Yet perhaps the most troubling use of predictive measures in counter terrorism is when it is meant for good, but still results in missteps or issues in the justice system. What happens when a reliance is built on such predictions, yet these predictions are unverifiable, or even wrong? The balance between protecting people's safety and their autonomy is a balance that many nations are struggling with, yet one that many people are not fully aware of.

Australia is a leader in preventative terrorism laws, which target potential criminals before they have a chance to commit crimes. Using intelligence to determine threats, Australia has implemented continuing detention orders and extended supervision orders, which The Guardian reports allow people to be imprisoned for three years or extensive supervision "on the basis of predicted crimes," even if they have not yet committed any crimes.

The use of predictive technology in Australia is not as politically motivated or even as pervasive as in other countries, but that does not mean it is perfect. Australia's system has made errors on multiple occasions that have resulted in the unfair or questionable treatment of many, some of whom are not even aware that the mistakes were being made.

In April of 2023, the government came under fire for their continued use of a tool that independent investigators reported they were very critical of, the Violent Extremism Risk Assessment 2 Revides (VERA-2R). According to The Guardian, the tool is used to assess whether or not extremists should be subject to strict court orders after their sentences, such as extended detentions or regular check-ins with police. A report by Drs. Emily Corner and Helen Taylor paid for by taxpayer money and submitted in May of 2020 found that "the lack of evidence" backing the tool had "serious implications for its validity and reliability." The report, however, remained largely undisclosed to lawyers and defendants for two years.

In the United States, predictive artificial intelligence has been known to solidify racial biases, rather than working to fix them.

According to the Australian government, the VERA system was designed to be used on individuals who had committed acts of extreme violence or acts related to terrorism, and as such were first used primarily in prison settings. As time has gone on, the system has been utilized in a much wider sense, expanding its use to those who might commit terrorist or extremist actions in the future. The validity of VERA-2R is also difficult to measure, as the information needed to do so is not widely published or available to the public. As such, research into its effectiveness and necessity is limited.

Yet that might not be the greatest flaw in the VERA-2R system. Earlier

Uyghur Muslims in conflict with police forces as China furthurs oppression of minority gorups.
Courtesy of Uyghur East Turkmenistan(flickr)

Australia's use of predictice technology has resulted in unfair or wrongful convictions. Courtesy of the public domain(rawpixel)

this year, it was found that the tool considered individuals as posing a greater risk of committing crimes if they were autistic or suffered from other mental illnesses, despite having no data-based reason to do so. A report released by the Australian government and academics at the Australian National University found that the tool was not "able to predict their specified risks with anything other than chance." While there was an attempt at recognizing and reconciling the issues, it was reported that the tools were used 14 times by the federal government after they were made aware of such issues.

> *...it was found that the tool considered individuals as posing a greater risk of committing crimes if they were autistic or suffered from other mental illnesses, despite having no data-based reason to do so.*

More than that, the federal government did not communicate these issues with the government of New South Wales, meaning that New South Wales continued to use results from this software to extend the monitoring and detention of individuals who had finished their sentences. Furthermore, once made aware of these issues, the New South Wales government did not alert the attorneys of those affected by the errors. When a potential threat is discovered, the Australian government holds the right to restrict the travel, work, and education of individuals, meaning that if falsely flagged, individuals' entire lives can be put on hold without a clear end date.

Hayley Le, a lawyer who represents a number of men assessed using the VERA-2R tool, told The Guardian that the New South Wales court did not share that it had the independent report regarding one of her clients. Le said that her client had not committed a terrorist action, and had possible mental health issues, as well as having faced circumstances that negatively impacted their reintegration into the community. As a result of findings based on the VERA-2R tool, Le's client was not allowed to leave the country or start any jobs, volunteer work, or education courses without the approval of the government. Only after the report was made clear to Le and her client did New South Wales offer to end its case for an extended supervision order for the client.

One of the main concerns with the extended supervision orders is that they do not seem to have the end goal of rehabilitation. The orders only keep their subjects out of the general population for a slightly extended period, and, as with Le's client, include stipulations that make it much harder for the subject to reenter the community once they have finished serving their sentences. Grant Donaldson, an independent national security legislation monitor, noted to The Guardian that while the intent of the orders was for the protection from and prevention of future terrorist activities, it "seemingly quite deliberately does not include rehabilitation or reintegration of the offender into the community." This idea, he concluded, was inconsistent with the intended purpose of sentencing, which include those two concepts as an important component, as well as disproportionate to the threats of terrorism.

With all of the issues surrounding its predictive tools and use of continued detention, Australia has faced some pushback. Human rights groups have pointed out that any false continuing detention orders would almost certainly amount to arbitrary detention under the International Convention on Civil and Political Rights, The Guardian adds. It also remains unclear whether the measures have actually done anything to prevent terrorist actions, with the home affairs department citing a number of attacks that occurred after the release of those convicted in places like England and Austria, while reports made by independent investigators say that there is no certainty to their efficacy. Yet the home affairs department maintains that the measures "provide for the management of terrorist offenders in custody and in the community," and does not plan on discontinuing their use.

> *It also remains unclear whether the measures have actually done anything to prevent terrorist actions...*

The fact that these errors can and do occur should be an issue that is concerning, even more so once one realizes how hard it is to know that they are happening. The clearance needed to understand the workings of this system and others like it is incredibly high, meaning that as these issues occur, it may take time for those affected by them to learn that they have been. These discrepancies in information create an environment where not only the outcome is uncertain, but the

King Street Courthouse, located in Sydney, Australia. Courtesy of Kgbo(Wikimedia Commons)

process is as well. As time goes on, the potential reach of such monitoring is unknown, as countries that are striving to prevent terrorist actions may extend limited measures beyond their current limitations and into other spheres.

The biggest issue faced in regulating the use of predictive technology is that it is inherently invasive. Defining the limit of how invasive a technology can be before it begins violating an individual's right to privacy is a slippery slope that creates contentious disagreement. While the right to privacy is important, governments and organizations, such as the United Nations, have stated that it is not absolute, though there has never been a decision made on just how far governments can extend their searches.

While the right to privacy is important, governments and organizations ... have stated that it is not absolute...

The intentions behind using predictive technology are not inherently bad in most cases. The desire to fight terrorism is noble, but as time goes on, the question of where "terrorism" begins is something that must be considered. Does it begin at the first concerning internet search, or perhaps the joining of an extremist group? As these events become easier to identify, what level of intervention is necessary to stop them? As technology advances from more simple predictive technology to the advanced artificial intelligence-based technology that is on the rise in many parts of the world, these questions will become much more poignant, and a definition will have to be decided upon.

Contact Sophie at sophie.ulm@student.shu.edu

How Paramilitary Power Struggles Shape the Terrorist Landscape in Northern Ireland

Kiara McGaughey | Staff Writer

Courtesy of Sinn Fein(Wikimedia Commons)

Northern Ireland has a long and complicated history of paramilitary activity, with groups displaying guerilla warfare and attacks of terror in public spaces. This history stems from the Troubles, a low-scale war that began in 1968 and continued until 1998. In the wake of Brexit, Northern Ireland has seen an increase of possible attacks, as well as regular paramilitary activity, in recent months.

Much of the media coverage surrounding current events unfolding in Northern Ireland focuses on the activities of dissident Republican paramilitary groups, such as splinter groups from the Irish Republican Army (IRA). Media coverage often focuses on events such as the groups' assassinations of political targets and bomb threats. However, recent activity from Unionist Protestant paramilitaries also deserves attention. The groups' parallel acts of violence and intimidation toward those they believe to be dissenters or, conversely, those they wish to recruit, as well as documentation of British collusion with the Unionist Protestant paramilitary groups during the Troubles, warrants increased media coverage.

The existence of Unionist Protestant forces in Ireland stems from the colonization of Ireland in the 12th century, when English and Scottish settlers gained control of the island. They established several "plantations" throughout Northern Ireland, most notably in Ulster, where they persecuted the native Irish predominantly through forced serfdom. After the Republic of Ireland gained independence, Irish-Catholics who controlled Northern Ireland wanted to unite with the Republic, whereas the Protestant inhabitants of Northern Ireland, mostly English and Scottish individuals who were involved in or descended from those involved in colonization, opposed the merger.

Protesters responded by forming the Ulster Defense Association (UDA) and Ulster Volunteer Force (UVF). These paramilitary groups sometimes conspired with the British army and the Ulster Defense Regiment (UDR), an arm of the British military. Recently declassified documents share that the groups supplied loyalist paramilitaries with UDR weaponry, encouraged dual membership of the UDR and UDA, and withheld information of UDR identity when trying a soldier in a loyalist paramilitary. These documents explain that most soldiers in the UDR also had joint memberships in loyalist paramilitary groups, working as UDR soldiers during the day and joining paramilitaries at night to help with war efforts or targeting and killing Irish-Catholics and those believed to be Republicans. After years of conflict, loyalist paramilitaries and Unionists signed the "Good Friday Agreement" in 1998, which declared that power was to be balanced by Unionists and Republicans in Northern Ireland's government, demilitarizing and effectively officially disbanding the organizations.

After the signing of the Good Friday Agreement, the UVF, UDA, and the IRA dissolved formally but continued activities as "splinter groups" and "gangs" which still act through many of the same activities as the original paramilitaries on a smaller scale. In post-conflict settings, splinter groups can become more subtle in their tactics yet more violent. Additionally, the Good Friday Agreement included no formal process of phasing out paramilitaries, which has allowed the UVF and UDA to, for the most part of the decade as well as during the Troubles, control territories and towns by use of force and intimidation. These splinter groups continue their acts of terrorism in an attempt to keep Irish nationalists out of certain areas and to intimidate or blackmail civilians into joining their organizations and help financially support them. According to locals and those anonymously involved with the UVF, "punishment attacks" still occur, in which anyone viewed as supporting or being involved with Irish nationalism or the IRA is beaten or threatened. Nationalists are also deterred from moving into territories with known Unionist activity and vice versa. Locals and business owners in these paramilitary territories must pay the organizations to not be continuously threatened.

Northern Ireland has seen an increase of possible attacks, as well as regular paramilitary activity, in recent months.

As a recruitment tactic, the UVF and UDA have begun money lending operations around food banks and charity centers, reportedly targeting disadvantaged people who cannot pay for essentials such as groceries and offering to lend them money. The loan operations are displayed at first as not being connected to the paramilitaries. However, the debts from the operations are described as nearly impossible to pay off, trapping individuals. The groups then show their paramilitary connections and force people into becoming members, asking them to protest with them and handle illegal exchanges such as funneling drugs. Victims' involvement further them into more illegal activity with less likelihood of escaping. It is also reported that paramilitary territory is most likely protected and fought over due to the exchange of drugs.

The occurrence of Brexit has also increased tensions in Northern Ireland, as terror attacks, assaults and threats have been more commonly reported since 2019, the year of Brexit's announcement. Both Republican and Unionist splinter groups have increased their public campaigns and made their objectives bolder.

In 2021, the UVF, UDA, and the Red Hand Commando renounced

Political unrest and violence have increased across Northern Ireland since Brexit's announcement in 2019.
Courtesy of Joshua Hayes(flickr)

their signing of the Good Friday Agreement. Under the Brexit deal, Northern Ireland remains within the European Union's (EU) market for goods, rather than within the UK's economy. The joint letter between the paramilitaries explains they do not want to reignite conflict but warn of "'permanent destruction' of the 1998 peace agreement without changes to post Brexit arrangements for Northern Ireland," according to The Guardian. The demands also face criticism as Irish Republicans feel Northern Ireland benefits most from the single EU economy.

Activity from paramilitary groups has also included an increase in violence. MI5, a group that monitors the terrorism risk in Northern Ireland, raised the terror threat to severe this April, meaning an attack was very likely. On April 10, the day before a visit from U.S. President Joe Biden, masked, dissident Republicans threw petrol bombs at a police car during a parade opposing the Good Friday Agreement. The week after, riots started to break out in Loyalist areas as protesters threw bricks and petrol bombs at police in response to the continued plans of Brexit's terms for Northern Ireland. NBC explains that Unionists feel that the Northern Irish and British police treat them more harshly than they do nationalists, as they unfairly side with nationalists. The notions were furthered when prosecutors chose not to press charges against members of the Sinn Fein party, a nationalist group, who attended the funeral of IRA leader Bobby Storey during COVID-era restrictions on mass gatherings.

> *MI5, a group that monitors the terrorism risk in Northern Ireland, raised the terror threat to severe this April, meaning an attack was very likely.*

Despite Union beliefs that the UK may be undermining their loyalism or citizenship, recent decisions such as amendments to the UK's Northern Ireland Conflict Bill, used originally to protect former British security from prosecution, have extended immunity toward former British soldiers including those in the UDR and police force responsible for crimes during the Troubles. The amendments of this bill, and knowledge that most in the UDR also have worked with loyalist paramilitaries, brings forth the worrying and overwhelming fact that loyalist groups and British colonization and control of Northern Ireland are connected intrinsically. British monitoring and countermeasures towards terrorism may be skewed in Unionist favor, despite the strong risk that Unionist paramilitaries create through territorial disputes and escalating conflicts with Republican groups. While the UK views both Unionist and Republican paramilitary groups as threats to the safety of the public, most British intelligence and media coverage focus on quelling dissident Republican groups, while viewing Unionist activity as less concerning. To create an effective response, intelligence in both Northern Ireland and the United Kingdom should view all paramilitaries as equal threats due to their ability to escalate conflicts, intimidate towns, and foster the creation and use of arms. Such intelligence may also be inherently swayed towards Unionist paramilitaries because of British collusion and interests of wanting Northern Ireland as an asset of the UK.

Contact Kiara at kiara.mcgaughey@student.shu.edu

The Sahel: Terrorism's Forgotten Front

Pranali Jain | Staff Writer

Courtesy of US Africa Command(flickr)

The term "terrorism" is often associated with the Levant region in Western Asia, also known as the Middle East – which is not surprising, considering the disproportionate focus that Western media places on terrorism in that region. However, while terrorism continues to be a global threat, in recent years, its epicenter has shifted to Africa – specifically in West Africa, the Sahel, and the Lake Chad Basin regions. The countries in these regions – Mali, Burkina Faso, Niger, Nigeria, Chad, and Cameroon – are major hotspots for terrorist operations. In 2021, 48 percent of all terrorism-related deaths across the world occurred in West Africa and the Sahel, according to Foreign Policy. Moreover, the UN reports that in 2022 alone, the continent witnessed 7,816 terrorism-related deaths. Despite the alarming proliferation of terrorism and terrorist activity on the continent, however, media coverage remains minimal.

The rise in terrorism in the Sahel region can be traced back to the fall of Muammar Gaddafi of Libya in 2011, which opened a power vacuum allowing arms to be transported across the region to terrorist cells affiliated with the Islamic State or Al-Qaeda in Mali and Burkina Faso. In the past 12 years, these terrorist groups have continuously taken advantage of the instability of the Sahel region and weakened states further. Over the last few years, a wave of coups and attempted coups in Burkina Faso, Chad, Mali, Guinea, and more recently, Niger, have been directly linked to the growing insecurity in the region due to the spread of terrorism. Niger's coup on July 23 was the ninth in a series of coups in West Africa. According to the leaders of the coup, their actions were in response to the state's worsening security and lack of substantial action against the jihadists. Similar reasoning has been provided by juntas of neighboring states to justify the coups.

The recent coup in Niger, a state that was considered an essential Western ally in the region against extremists and one of the last beacons of democracy in the Sahel, only deteriorates the situation and further complicates counter-terrorism efforts. Western governments, the United Nations, and the African Union have presented Nigerien coup leaders with an ultimatum – either restore civilian control or face a series of sanctions. The French government has also suspended budgetary support and the United States has halted all security operations within Nigerien borders. This has led Niger and other states facing similar Western rebukes to turn to Russia's Wagner Group, a private military company affiliated with Russian President Vladimir Putin and notorious for human rights abuses and exploitation, to fill in the gaps in security left by Western militaries. Simultaneously, terrorist groups in the region are also taking advantage of the fragile situation and are exploiting the security gaps to grow their organizations as foreign powers withdraw.

In 2021, 48 percent of all terrorism-related deaths across the world occurred in West Africa and the Sahel

The combination of exploitative entities has exacerbated the dire humanitarian conditions and political instability in the region. The recent coups have further initiated an endless cycle of growth for terrorist activity. Acute food insecurity and an increase in human displacement, amongst other issues, are the immediate consequences of the rise of extremist violence and democratic regression within the region. And with suspended foreign aid and support, the socioeconomic conditions in Niger, Mali, and the Sahel as a whole, will worsen.

The deteriorating socioeconomic conditions in West Africa and the Sahel are one of the main reasons why terrorism is able to grow rapidly and flourish within the region. High unemployment rates, hunger, lack of basic services, and the constant volatility in the political sphere have forced civilians to resort to desperate measures to procure basic needs. In other words, the dire socioeconomic situation has simplified recruitment for terrorist groups operating in the region. Terrorist groups are able to draw recruits with the promise of providing them with basic necessities and protection – something the governments in the region have failed to provide. Studies by the UN Development Program show that 25 percent of recruits were experiencing unemployment at the time of recruitment, and almost 40 percent of recruitsts claimed they joined as a means to meet basic necessities. For example, in Nigeria, the main terrorist organization – Boko Haram – recruits students from poor families in the poverty-stricken areas of Northern Nigeria.

Terrorist groups in the region are also taking advantage of state insecurity and political instability to fund their organizations and strengthen their foothold in the Sahel through illegal means. These groups are known to traffic drugs and minerals, organize kidnappings for ransom, and engage in other illegal activities to support their operations – all of which are made easier during a time of weak governance and political crises. The already dire socioeconomic circumstances of the Sahel, coupled with the recent coups, have laid fertile ground for terrorism to flourish at an alarming rate in the region. As Wagner's presence grows, the circumstances in affected states are only expected to get worse.

Counter-terrorism efforts in the region have usually focused primarily on strengthening security and consisted of military training and aid from Western governments. For instance, the annual Flintlock event, held this year in Ghana and Ivory Coast, is a U.S.-led military special training exercise for West African militaries and law enforcement to help combat extremist violence. Similar approaches have been enacted by the French government and other African governments in attempts to stabilize the region and diminish terrorist violence. Yet, counter-insurgency measures that have solely focused on military operations have proven to be unsuccessful.

Security-driven responses to combat terrorism hardly address the socioeconomic drivers of terrorism and related instability in the region. Governments and organizations need to invest more time and resources to address the root causes of extremist violence and tailor counterterrorism approaches specific to the Sahel region. Investment and support must be directed toward developmental solutions that seek to minimize or resolve the high unemployment rates, lack of education and access to basic needs, poverty, and food insecurity. Security-focused approaches, although important, have proven to be costly, inadequate, and, at times, worsened the situation altogether.

Counter-insurgency measures that have solely focused on military operations have proven to be unsuccessful.

In order to successfully curb the proliferation of terrorism in the region, governments also need to employ a bottom-up approach and invest in developmental efforts that put communities at the center of the post-conflict healing process and counter-terrorism efforts. For example, community rebuilding and healing services that focus on mental health in Rwanda, Kenya, and the Lake Chad Basin region post conflict has helped reduce the recidivism of defectors and forced recruits. Programs that focus on socioeconomic development, education, and employment are also drastically expected to stabilize communities and improve prevention records. It should be noted that programs such as Flintlock have an international law and "humane war" component to them, which urge militaries and law enforcement of participating states to value civilian life and conduct war in accordance with international law. Nevertheless, they still fail to actually address the root causes of terrorism's expansion in the region.

Additionally, the enforcement of economic sanctions in response to the recent coups will only exacerbate the poor socioeconomic state of the affected region, placing additional pressure on communities to resort to unsavory means of survival. Hence, governments not only need to strike a delicate balance between allocating resources between security and developmental approaches to combat terrorism in the Sahel, but also between punishing insurgents and coup leaders while safeguarding civilian needs.

As the Sahel region continues to serve as a hotbed for terrorist activity, governments and international organizations are failing to address the root causes of the rapid expansion of insurgency in the region. As the region steadily succumbs to insecurity and political instability due to a lack of successful counterterrorism efforts, the situation continues to worsen as terrorists and other exploitative groups have strengthened their presence. With each day, it becomes imperative that the current counter-terrorism paradigm shift to accommodate the region's socioeconomic needs to combat extremism successfully.

Contact Pranali at pranali.jain@student.shu.edu

Senegalese soldiers participate in shooting drills as part of operations. Courtesy of US Africa Command(flickr)

The Diplomatic Envoy

Courtesy of US Africa Command(flickr)

The Diplomatic Envoy

The Official Undergraduate Foreign Affairs Paper of Seton Hall University's School of Diplomacy

facebook.com/diplomaticenvoy

@EnvoyatSHU

@EnvoyatSHU

blogs.shu.edu/thediplomaticenvoy

thediplomaticenvoy@gmail.com

Follow us for the latest news, and scan the code to write for us!