Katarzyna Maniszewska
Monika Nowicka
Paulina Piasecka
Vanessa Tinker Editors

SECURITY AND SOCIETY

IN THE INFORMATION AGE

Volume 8

SRAS
Uniwersytet Civitas

Katarzyna Maniszewska
Monika Nowicka
Paulina Piasecka
Vanessa Tinker Editors

SECURITY AND SOCIETY

IN THE INFORMATION AGE

Volume 8

SRAS
Uniwersytet Civitas

Warsaw 2025

CIVITAS UNIVERSITY

Reviews:
Szlachter Damian, PhD, Polish Association of National Security
Tomasz Serafin, PhD, Pomeranian University of Applied Sciences in Starogard Gdanski

Editors:
Katarzyna Maniszewska, PhD (https://orcid.org/0000-0002-8021-8135)
Monika Nowicka, PhD (https://orcid.org/0000-0002-0430-8251)
Paulina Piasecka, PhD (https://orcid.org/0000-0003-3133-8154)
Vanessa Tinker, PhD (https://orcid.org/0000-0003-0955-4299)
Proofreader: Vanessa Tinker, PhD

ISBN print: 978-83-66386-60-0
e-ISNB: 978-83-66386-61-7

DOI: 10.6084/m9.figshare.30619181

Publisher: Civitas University Press
Palace of Culture and Science, XI floor
00-901 Warsaw, 1 Defilad Square
tel. +48 22 656 71 96
e-mail: wydawnictwo@civitas.edu.pl
http://www.civitas.edu.pl

Typesetting and text makeup:
Magdalena Giera | Magio | magio.pl

Contents

Preface

We are pleased to present the eighth volume, bringing together a unique series of papers by talented young researchers from both sides of the Atlantic. This publication includes articles by "Security and Society in the Information Age" program participants and papers by International Security Studies students, presenting the transatlantic youth perspectives on security issues.

The "Security and Society in the Information Age" program, composed of a summer school and semester/academic year study abroad opportunities, was designed and launched jointly in 2015 by two partners: SRAS (USA) — a leading study abroad facilitator, and Civitas University (formerly: Collegium Civitas) — a leading non-public university in Warsaw, Poland.

The summer school combines a four-week intensive course on Central Europe & Security Issues with a two-week research internship with the Terrorism Research Centre at Civitas University. The program offers a distinctive opportunity to explore global security challenges through the historical, political, and cultural lens of Central Europe.

The 2025 curriculum focused on new and emerging threats, including the regional and global consequences of the Russian invasion of Ukraine and the broader interconnectedness of international conflicts, with special attention to developments in the Middle East. During the 2025 summer school 19 participants — students of leading American colleges and universities — engaged deeply with critical topics such as terrorism and counterterrorism strategies, state sponsorship of terrorism, radicalization and prevention, public diplomacy, private military companies, international

humanitarian law, peacebuilding and post-conflict reconstruction, hybrid threats and disinformation, and cybersecurity.

Those topics are reflected in this book. In addition, students and alums of the International Security Studies master's degree program at Civitas University were invited to submit papers to this volume. By gathering youth perspectives on security issues, from Europe and the US, with this book, we hope to contribute to strengthening the transatlantic bonds in security research, primarily among the new generation of researchers.

We hope you will find the perspectives gathered in this book interesting, and we invite you to learn more about the study abroad and summer school program "Security and Society in the Information Age" at www.securityandsociety.org.

Dr. Katarzyna Maniszewska
Summer School Director
Civitas University

Dr. Paulina Piasecka
Director
Terrorism Research Center

Renee Stillings
Director
SRAS

PART I

SECURITY AND SOCIETY

1

Sowing Seeds of Discord: Russian Attempts to Weaken US Commitment for NATO Via Disinformation Campaigns

Andrew ELLIS

Abstract: This article examines Russian disinformation campaigns targeting the United States, with a focus on the evolution of their tactics and efforts to weaken public commitment to NATO. Using the 2016, 2020, and 2024 U.S. elections as case studies, the article analyzes how Russian strategies have adapted over time to exploit political divisions and digital platforms. It also evaluates Russian anti-NATO operations within this broader context. The final section discusses current countermeasures taken by the United States and other Western democracies and offers recommendations for strengthening resilience against future disinformation threats.

Keywords: Russia, Russian Federation, United States, NATO, alliance disinformation, disinformation campaigns, US elections, hybrid warfare

Introduction

The North Atlantic Treaty Organization (NATO) has been a cornerstone of democratic security since its founding in 1949. The ongoing war in Ukraine underscores NATO's continued relevance in deterring authoritarian aggression. While the Kremlin publicly portrays its opposition to NATO as a reaction

to the alliance's eastward expansion, many analysts contend that Russia's deeper concern lies in NATO's ability to obstruct its regional ambitions and promote democratic norms that challenge authoritarian regimes. This suspicion toward NATO is not new; the Soviet Union held similar views during the Cold War. In its analysis, the U.S. Department of State debunks several of the Kremlin's key disinformation narratives, including Vladimir Putin's claim that Russia is liberating Ukraine from "drug addicts and neo-Nazis," and that NATO's growth left Russia no choice but to invade.[1] As Foreign Service Officer Ken Moskowitz argues, Putin's hostility toward NATO stems from his belief in Russia's right to a "sphere of influence."[2] By framing NATO as a threat to Russian sovereignty, the Kremlin uses disinformation — such as fabricated neo-Nazi conspiracies and false claims of NATO expansionism — to mask Putin's broader imperialist objectives.

An additional possible reason for Putin's anti-NATO stance is that NATO is a pillar of Western democratic cooperation. The collapse of the Soviet Union in 1991 was, in part, the result of democratization within its sphere of influence — a process Putin viewed firsthand. He later described the Soviet Union's dissolution as "the greatest geopolitical catastrophe of the 20th century".[3] For an authoritarian like Putin, the existence and success of nearby democracies pose an ideological threat to his regime. Ukraine exemplifies this threat. During the 2013 Euromaidan movement, Ukrainians staged mass protests against then-President Viktor Yanukovych after he aligned with Moscow, exposing rampant corruption.[4] The protest movement successfully ousted Yanukovych, signaling Ukraine's push for democratic independence and weakening Russia's influence in the region. In response, Russia annexed Crimea in 2014 — a connection highlighted

---

[1] U.S. Department of State, "Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War," accessed August 5, 2025, https://2021-2025.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war.

[2] Ken Moskowitz, "Did NATO Expansion Really Cause Putin's Invasion? A Seasoned Diplomat Considers This Question in Light of His Own Experience," *Foreign Service Journal*, October 2022, accessed August 5, 2025, https://afsa.org/did-nato-expansion-really-cause-putins-invasion.

[3] Miguel Vázquez Liñán, "History as a Propaganda Tool in Putin's Russia," *Communist and Post-Communist Studies* 43, no. 2 (2010): 167–78, https://www.jstor.org/stable/48609753.

[4] Nadia Diuk, "Euromaidan: Ukraine's Self-Organizing Revolution," *World Affairs* 176, no. 6 (2014): 9–16, http://www.jstor.org/stable/43555086.

by Lt. Col. Robert J. Moschella in an Air War College report.[5] This pattern continued in 2022 with Russia's full-scale invasion of Ukraine, underscoring Putin's broader effort to suppress democratic movements near Russia's borders.

While Ukraine remains the primary target of Russia's aggression, the democracies supporting Ukraine — many of them NATO members — are also under attack through non-military means. According to a NATO review on hybrid warfare, "hybrid warfare entails an interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion".[6] Although the concept has been critiqued for its vagueness, it is nonetheless useful for understanding how states can undermine adversaries without engaging in open conflict. This applies to the current situation in Europe, as Russia continues its invasion of Ukraine militarily alongside non-conventional means against Ukraine and Ukraine's allies (NATO members). Hybrid warfare is enticing to many aggressor nations because it offers an opportunity to attack rivals without the risks of conventional war. As the NATO Review notes, "[t]he costs and risks are markedly less, but the damage is real".[7] These tactics may include economic pressure, cyberattacks, disinformation campaigns, and even the support of terrorist or separatist groups — all of which allow hostile states to weaken opponents without firing a single shot.

This paper investigates how the Kremlin uses foreign information manipulation and interference (FIMI) campaigns to undermine support for NATO within U.S. democratic institutions and civil society. The U.S. Government Accountability Office (GAO) defines foreign disinformation as "false claims or misleading information deliberately created or spread by foreign actors to deceive people," often with the goal of destabilizing

---

[5] Robert J. Moschella, *The Besieged Fortress: Making Sense of Russia's Annexation of Crimea and What It Means to U.S. Policy Makers*, Defence Technical Information Center, accessed August 5, 2025, https://apps.dtic.mil/sti/citations/AD1038278.

[6] NATO Review, "Hybrid Warfare — New Threats, Complexity, and 'Trust' as the Antidote," last modified November 30, 2021, accessed August 5, 2025, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

[7] *NATO Review*, "Hybrid Warfare."

democracies.[8] A FIMI campaign refers to the sustained and strategic use of such tactics, commonly seen in Russian operations. Drawing from the hybrid warfare framework — which views disinformation as a non-military tool of subversion — the study examines how these campaigns erode public trust in democratic processes, destabilize alliances, and promote Russian geopolitical interests without conventional military conflict. The following research questions guide the analysis: How does the Kremlin employ disinformation to weaken U.S. public confidence in elections and foreign policy, particularly regarding NATO? What strategies has NATO employed in response, and what more can be done to counter these threats? The paper uses a qualitative content analysis of government documents, policy reports, and academic studies to trace evolving disinformation tactics and assess their impacts. Case studies include Kremlin interference in U.S. elections and NATO-aligned states such as Bulgaria[9], where pro-Russian political narratives have been amplified through media manipulation and social division. Ultimately, this study argues that Kremlin-backed disinformation campaigns represent a strategic effort to weaken democratic resilience and fracture international security cooperation.

Russian Disinformation

The Kremlin does not recklessly spread falsehoods; rather, it employs a calculated strategy and a set of evolving tactics to achieve its manipulation objectives. These disinformation methods are continually refined to increase their effectiveness and evade detection. As noted by Joseph W. Robbins in a report for the Center for Strategic and International Studies (CSIS), the Kremlin's success lies in its ability to constantly adapt and

---

[8] U.S. Government Accountability Office, *Foreign Disinformation: Defining and Detecting Threats*, GAO-24-107600 (Washington, DC: GAO, 2024), 1, accessed June 27, 2025, https://www.gao.gov/assets/gao-24-107600.pdf.

[9] Rumena Filipova, "The Kremlin's Agenda in Bulgaria: The Role of Pro-Neutrality Protests in Disinformation Campaigns," in *Hacking Minds and Machines: Foreign Interference in the Digital Era*, ed. Nad'a Kovalčíková (Paris: European Union Institute for Security Studies, 2024), 5, https://www.jstor.org/stable/resrep62147.5.

evolve its tactics.[10] The Kremlin's objectives include undermining democratic cooperation by weakening commitment to NATO and eroding U.S. foreign policy resolve, as evidenced in the Doppelganger disinformation campaign discussed below. Weakened commitment to NATO directly benefits the Kremlin, as it reduces opposition to Russian expansionism in Ukraine and potentially other post-Soviet states within Putin's envisioned sphere of influence. Moreover, Putin's regime is more secure when democracy is fragile elsewhere; it allows him to frame authoritarianism as a source of strength and stability, in contrast to what he portrays as the chaos and weakness of democratic governance. Given this opportunity, Putin can more easily suppress democratic movements within Russia by pointing to instability abroad. The Kremlin's disinformation strategy is designed to promote polarization, sow distrust in democratic institutions, and undermine confidence in the media, political discourse, and electoral systems — tactics reflected in the Doppelganger campaign discussed below. In essence, the objective is simple: destabilize democracy by eroding public trust and national cohesion. The Kremlin uses a constantly evolving arsenal of tactics to do this, including direct interference in elections, using AI-generated deepfakes, manipulating influencers into spreading their narratives, identity theft of individuals (such as politicians) or organizations (such as new agencies), and creating fake versions of websites or platforms for the dissemination of disinformation. Russian authorities have developed a multichannel disinformation strategy designed for maximum impact. As Robbins notes, the Kremlin's use of coordinated "troll factories" enables the mass production and rapid dissemination of disinformation across multiple platforms simultaneously.[11] A military volley is an old, but still used method of using projectiles en masse. One of the reasons for this tactic is inciting the most shock, panic, and chaos as possible among the enemy, an attack on their morale and organization, which then hinders their response power if effective. The Kremlin's FIMI volley works in a similar way, using all of their disinformation methods in synchronized and concentrated full

[10] Robbins, "Countering Russian Disinformation."

[11] Ibid.

force, attempting to damage United States (and other target's) societal morale and organization through shock and chaos.

2016 and 2020 Presidential Elections

Three major examples of Russian FIMI campaigns against the United States include: the 2016, 2020, and 2024 presidential elections. Beginning with 2016, Russian tactics focused mainly on direct interference in the election process. Twelve Russian intelligence agents were indicted by a federal grand jury for interfering with the 2016 presidential election, as found in an FBI investigation. The report states: "[t]he indictment charges 11 defendants… 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", along with other crimes committed in the process, such as money laundering and identity theft.[12] The report further mentions how two of the twelve Russian agents were "charged with a separate conspiracy to commit computer crimes, relating to hacking into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections".[13]

These acts constitute serious violations of U.S. law and clear intrusions into the electoral system. Notably, the charges reflect two distinct tactics: influencing public perception through document leaks and media manipulation, and interfering directly with election infrastructure. The National Intelligence Council defines election influence as "overt and covert efforts by foreign governments or actors acting as agents of, or on behalf of, foreign governments intended to affect directly or indirectly a US election

[12] Federal Bureau of Investigation. *Russian Interference in 2016 U.S. Elections*. Accessed June 19, 2025. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

[13] Ibid.

— including candidates, political parties, voters or their preferences, or political processes", while "[e]lection interference is a subset of election influence activities targeted at the technical aspects of the election, including voter registration, casting and counting ballots, or reporting results".[14] Both serve the Kremlin's ultimate goal: to install a favorable candidate and weaken democratic institutions. In 2016, Russian operatives engaged in both influence and interference efforts to support Donald Trump's candidacy, hoping he would undermine the United States' commitment to NATO and weaken its foreign policy resolve.

In the 2020 elections the Kremlin released another volley of disinformation against the United States. Here the National Intelligence Council found no evidence of Russian direct interference, only malign influence. The National Intelligence Council reports Kremlin "influence operations aimed at denigrating President Biden's candidacy and the Democratic Party, supporting former President Trump, undermining public confidence in the electoral process, and exacerbating sociopolitical divisions in the US".[15] The report further emphasizes that the Kremlin worked with proxy actors — some of whom were closely linked to former President Trump and his administration — to spread rumors and false narratives aimed at defaming Joe Biden during his presidential campaign.[16] Some of these rumors are backed by fake videos/images (deepfake) and conspiracies of election fraud by the Democratic Party.[17]

Although the Kremlin's tactics have evolved, its core strategy, objectives, and preferred candidate have remained consistent. In recent election cycles, Russian operations have shifted toward more covert influence campaigns, aiming to erode American faith in democracy without drawing direct attention to their malign activities. Heather A. Conley of the

---

[14] National Intelligence Council. *Foreign Threats to the 2020 US Federal Elections*. Office of the Director of National Intelligence, March 16, 2021. Accessed June 19, 2025. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

[15] Ibid.

[16] Ibid.

[17] Bryan Nakayama, "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations," *The Cyber Defense Review* 7, no. 3 (2022): 49–66, https://www.jstor.org/stable/48682322.

Center for Strategic and International Studies (CSIS) argues that the first step in countering Russian disinformation is acknowledging that "we are at war."[18] She contends that "if the American people understood that we are facing a new kind of war, a greater sense of patriotism and duty about what is at stake would be awakened," drawing a parallel to the surge of unity following the attack on Pearl Harbor.[19] Though written in 2019, Conley's warning remains highly relevant. If more Americans understood the scope of Russia's foreign information manipulation and interference (FIMI) efforts — and their role in exacerbating domestic polarization — it is likely that public response would be more unified and resolute.

Aware of this risk, the Kremlin has adapted its strategy to prioritize influence over direct interference, staying under the radar while continuing to shape public opinion and weaken democratic institutions. Even though the campaign failed to get Trump elected, it still impacted the American faith in United States democratic processes. While the Kremlin may not have achieved all its immediate goals, it effectively laid the groundwork for future destabilization. Arguably the 2020 Russian FIMI degraded this trust more than the 2016 campaign, if you take into account the January 6th storming of the Capital as further destabilizing and representing a further polarizing American society. The Kremlin did not reap full fruits from this campaign, but laid the groundwork for the next.

2024 Presidential Election and NATO

The name for Russia's disinformation campaign influencing the 2024 election was referred to as "Doppelganger" by the FBI. This campaign displayed further Russian tactical adaptation and improvement. In this case, as a Justice Department release indicated, the Kremlin went through Russian companies, such as SDA (Social Design Agency), Structura,

---

[18] Heather A. Conley, *Undermining Democracy: Kremlin Tools of Malign Political Influence*. Center for Strategic and International Studies (CSIS), 2019. https://www.jstor.org/stable/resrep37610.

[19] Conley, *Undermining Democracy*.

and Dialog.[20] The report then explained that through these companies, the Kremlin funded and organized a multi-layered, cross-platform, campaign. This effort made prevalent use of AI to generate content such as deepfakes and narratives. The operation, as outlined by the Justice Department, relied on three seized Russian documents discussing the three pronged operation, with the Russian names of "Good Ole USA Project", "The Guerilla Media Campaign", and the "US Social Media Influencers Network Project".

The goal stated in the Good Ole USA Project document is to secure Trump or Republican victory in the elections.[21] While the FBI redacted the names of specific politicians and parties — referring to them instead as "Candidate A" or "U.S. Political Party B" — the context and associated political views make their identities relatively clear. The Good Ole USA Project aimed to shift American public opinion on several fronts. One goal was to raise the percentage of Americans who believed the U.S. was "doing way too much to support Ukraine" from 41% to 51%. Another objective was to increase the share of respondents who agreed that the war in Ukraine should be ended as soon as possible — even if it meant ceding territory to Russia — from 43% to 53%. Finally, the campaign sought to reduce confidence in a prominent political figure — referred to in the report as "Candidate B," likely either President Biden or Vice President Harris depending on the timeline — from 39% to no more than 29%.

To achieve its objectives, the project targeted specific populations, such as swing states and Hispanic populations, via social media platforms. The document states plainly that these channels "will have extensive viral content — music, humor, beautiful girls, etc." to draw in viewers.[22] Russians also used channels disguised as American media outlets to

---

[20] U.S. Department of Justice. *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*. Press release, July 11, 2023. Accessed June 16, 2025. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.

[21] U.S. Department of Justice. *The Good Ole USA Project*. Accessed June 20, 2025. https://www.justice.gov/archives/opa/media/1366201/dl.

[22] Ibid.

distribute deepfakes, redubbed videos, and other forms of manipulated content. These channels operated in a "sleeper state," avoiding overtly political content while building a loyal following. As elections approached, they shifted strategies — using targeted ads and posts to promote other Russian-run channels that focused on political messaging and distributed pro-Russian disinformation. This project also involved working with American influencers who shared conservative values and were likely to agree with — and amplify — Russian narratives, such as withdrawing support from Ukraine or normalizing U.S.–Russia relations.

The next prong, the Guerilla Media Campaign, focused on targeting Republicans and poor whites with carefully disguised disinformation on social media platforms, adding fuel to existing citizen demands to withdraw from foreign affairs to focus on internal affairs. The Russian planners prey on the already existing conservative American fears of "new globalist socialism" (American left), with claims of "reverse discrimination" and loss of "The American Dream".[23] The campaign fueled Republican concerns that the U.S. was overspending on Ukraine while neglecting domestic economic issues — particularly the fear among working-class white Americans that such spending would threaten their jobs and increase the cost of living, a theme prominently noted in the document.

To manipulate these sentiments, Russian operatives created content disguised as American media, often mimicking outlets like Fox News. They used comments, videos, memes, and group chats to disseminate this material as broadly as possible. The operation relied on organized production teams responsible for generating high volumes of content and monitoring audience reactions.

Importantly, the planners emphasized on producing maximum content and monitoring the channels and advising the production teams. The planners emphasized in the document the importance of "use[ing] a minimum of fake news and a maximum of realistic information", and when fake news is used, the importance of "continuously repeat[ing]

[23] U.S. Department of Justice. *Guerilla Media Campaign in the United States*. Accessed June 20, 2025. https://www.justice.gov/archives/opa/media/1366196/dl.

that this is what is really happening, but the official media will never tell you about".[24] This strategy highlights the high level of organization and sophistication of the Russian operation, compared to previous Russian FIMI campaigns. It also highlights the growing threat of Russian malign influence, particularly the shift toward more sophisticated disinformation. While blatantly fake news is easier to identify, disinformation becomes far more potent when it blends mostly accurate information with subtle lies and biased framing.

Ultimately, the *Guerilla Media Campaign* was a key pillar in Russia's effort to influence American minds ahead of the 2024 election. Though the tactics evolved, the objective remained unchanged: erode trust in democratic institutions, stoke division, reduce support for global engagement, and push the United States toward a posture more favorable to Putin.

The third prong of Doppelganger was the US Social Media Influencers Network operation. This prong focused on creating fake American accounts and relied less on spreading disinformation than on simply advancing Republican narratives that aligned with Russia's. The report explained that the operation created and maintained approximately two hundred accounts in total, with two "active accounts" and two "dormant accounts" assigned to each state. The active accounts posed as individuals who supported the Republican Party or represented communities of local activists, and they posted, reposted, and commented in support of narratives shared by both Republican and Kremlin-aligned sources. The dormant accounts were created as backups in case the active accounts were blocked, continuing to further the Kremlin's agenda — though with less activity. Dormant accounts were a failsafe response to increased cooperation between Meta and the National Security Agency (NSA), which was identified as an obstacle to the operation. X (formerly Twitter) was also mentioned as a platform better suited for the campaign, though the report notes that X's fact-checking programs posed their own challenges. Additionally, Russian planners used American VPNs for these accounts as a further measure to evade U.S. defenses.

[24] U.S. Department of Justice, *Guerilla Media Campaign*.

The U.S. Social Media Influencers Network operation shared some tactical similarities — and differences — with the other two 2024 operations. However, the strategy and objectives remained consistent: to undermine the American democratic process (with media as a central target), promote polarization, reduce support for an internationally engaged United States, and push the country toward greater alignment with Russian conservative ideals.

Russian anti-NATO malign influence is another case crucial to this discussion. Kremlin FIMI undercuts American commitment to NATO by directly attacking NATO's reputation, not just by attacking general American commitment to strong foreign policy. For example, some of the Doppelganger narratives attempted to defame NATO by spreading disinformation about it as an aggressor in Ukraine.[25] NATO's official website was even among the victims of Doppelganger site-mimicking, as the Russians created the "'nato[.]ws' domain" which "was used to mimic the official NATO website for credibility and spread false press releases", such as announcing that NATO is considering "deploying Ukrainian paramilitary troops to France to 'suppress' protests".[26] These mimic sites even include links to the real home page for increased credibility, according to USCYBERCOM.[27] The Kremlin claims that NATO is an aggressor and pulls its' members into a war they do not want to be in. Russia disseminates this narrative via disinformation campaigns such as Doppelganger. The Russian disinformation does not stop at victims in immediate contact, but spreads like a disease, relying on Americans to further disseminate the disinformation for them, including disinformation defaming NATO. This will be discussed further later.

---

[25] U.S. Cyber Command. *Russian Disinformation Campaign "DoppelGänger" Unmasked: A Web of Deception*. June 6, 2024. Accessed June 16, 2025. https://www.cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception.

[26] G. Bergmanis-Korāts, M. Isupova, and R. R. Vecmanis, *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty* (Riga: NATO Strategic Communications Centre of Excellence, 2025).

[27] U.S. Cyber Command, *DoppelGänger: A Web of Deception*.

The Stakes of Disinformation

The Kremlin's FIMI campaigns pose a serious threat to both the internal health of democratic systems and the cooperation between democratic states — particularly in the area of defense. Disinformation undermines public trust, weakens democratic institutions, and erodes national sovereignty. Because democracies are inherently more transparent and pluralistic, they are more vulnerable to manipulation. Kremlin disinformation exploits these vulnerabilities, amplifying existing divisions and uncertainty. If democratic nations fail to confront this threat collectively, they risk being isolated, weakened, or destabilized one by one. NATO makes western democracies stronger through their mutual cooperation and trust, which is why Putin is attacking commitment to NATO. The sovereignty of individual democratic nations, including the United States is also defiled continuously by Kremlin disinformation. Vladimir Surkov, one of Putin's advisors, stated in 2019: "Foreign politicians talk about Russia's interference and referendums around the world. In fact, the matter is even more serious: Russia interferes in your brains, we change your conscience, and there is nothing you can do about it".[28] This quote encapsulates the breaches of sovereignty the Kremlin prides itself on for getting away with. The quote also displays the growing threat discussed earlier, as Kremlin disinformation tactics evolve to be more potent and difficult to block. The GAO clearly refers to disinformation as a "[threat] to U.S. national security".[29] If action is not taken now to orient defenses to Russia's latest capabilities and campaigns, the Kremlin (and other leading malign influence actors, such as Iran or China) will be able to continue manipulating democratic societies and politics unchallenged.

Responses

The United States, many European countries, and NATO are responding to Russian malign influence with countermeasures. Cyber threat intelligence expert, Dr. Bryan Nakayama discusses measures taken by the United States,

[28] Conley, *Undermining Democracy*, 12.

[29] U.S. Government Accountability Office, *Foreign Disinformation*, 1.

United Kingdom, France, and Germany as of 2022. Of these countries France has the most aggressive response. France integrated counter-disinformation teams into their cyber branch of the military and implemented media accountability legislation.[30] Integrating counter-disinformation teams into the cyber defense force helps by systematically addressing disinformation attacks as a threat, which is the first step and serves as a base on which to build a defense. According to Nakayama, French media accountability legislation emphasizes enhanced monitoring by requiring social media platforms to implement a tool that allows users to flag suspected disinformation, which is then investigated and removed if verified.[31] It also holds media platforms accountable to delete disinformation in "as little as one hour's notice". Germany, the United Kingdom, and the United States also responded by creating counter-disinformation teams and integrating them into cyber-defense parts of the military. Nakayama also discusses the United Kingdom's approach of implementing media literacy into education programs and expanding "[i]nformation operations" in cooperation with NATO, supporting "NATO operations by defending against false or exaggerated narratives".[32]

Senior Analyst at the EU Institute for Security Studies, Dr. Andrea Salvi proposes some possible solutions in his article focused on deep fakes. His main argument advocates as much cross-collaboration as possible, or "a comprehensive and agile response strategy with engagement from the broader multi- stakeholder community".[33] This multi-stakeholder community includes "[p]olicymakers, IT specialists, researchers and civil society members", who need to increase monitoring and work to secure the "information and cybersecurity ecosystem. Salvi includes the European Union as an example of this cross-collaboration, discussing how the

---

[30] Bryan Nakayama, "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations," *The Cyber Defense Review* 7, no. 3 (2022): 49–66, https://www.jstor.org/stable/48682322.

[31] Nakayama, "Democracies and the Future," 51.

[32] Ibid.

[33] Andrea Salvi, "The Attack of the Clones: Deepfakes and the Evolving Landscape of Disinformation," in *Hacking Minds and Machines: Foreign Interference in the Digital Era*, ed. Nad'a Kovalčíková (Paris: European Union Institute for Security Studies, 2024), https://www.jstor.org/stable/resrep62147.7.

European Union created and updates a Code of Conduct for the information environment, with the support of civil society and big tech companies. This Code of Conduct and Digital Services Act "establishes severe penalties for disinformation as well as fines for platforms that fail to comply with the obligations" and requires platforms to "demonstrate their procedures for reporting and taking down illegal content as well as content identified as information manipulation".[34]

The NATO Virtual Manipulation Brief 2025 provides a thorough analysis of where Russia's (and other malign actors') disinformation capabilities stand, their increasing use of generative AI, and ideas for defensive response. According to the report, "the Kremlin-aligned information space heavily relies on amplification," for which the Russians rely on reposts and audience engagement.[35] The report explains how content on platforms like X tend to have more reposts, but content on platforms like Telegram and YouTube tend to garner more audience engagement (such as comments or individual related posts). Both of these kinds of platforms help to spread Russian narratives and having two general platform routes helps insure Kremlin narrative amplification. The NATO brief also emphasizes Russia's growing use and investment in AI to create content faster and more convincing as well as "coordinate generative AI agent swarms", as mentioned above, through systems, such as Model Context Protocol (MCP), that standardize modes of communication between different kinds of AI.[36]

In response, the NATO report provides a plan for countering the next Russian threat. Because Russian tactics are constantly evolving, it is not enough to only learn how to counter the tactics used in the past. This plan centers defense around establishing a prediction system, bolstering rapid response capabilities, and reducing disinformation's effect on society. NATO's report suggests establishing a prediction system via fostering "the ability to forecast virality and evaluate the immediate and long-term

---

[34] Ibid.

[35] G. Bergmanis-Korāts, M. Isupova, and R. R. Vecmanis, *Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty* (Riga: NATO Strategic Communications Centre of Excellence, 2025), 6.

[36] Ibid., 26.

effects" of FIMI on society, mentioning audience behavior models as a tool to help achieve this.[37] Monitoring and analyzing media trends and Russian cross-platform coordination also help to keep updated on the latest threat capabilities, which is essential to forecasting attacks and tactics.

For the second part of the plan, the briefing recommends coupling "narrative-environment map[s]", which track and analyze disinformation "bursts" and societal vulnerabilities, with "agile rapid-response cell[s]".[38] In essence, this means fostering greater cooperation between systems working to analyze attacks and systems working to patrol platforms. Like watchmen in the towers, those monitoring threats must clearly communicate with the guards on the walls and within the fort — alerting them when, where, and how an attack may come so they can prepare and defend accordingly. The report concludes by recommending public awareness campaigns to strengthen societal resilience to FIMI, acknowledging that some disinformation will inevitably bypass even the most robust defenses. Given the high speed environment created by the information age and AI, prediction and rapid response are the only way to intercept Russian disinformation volleys. At the same time, building public resilience is critical for countering the disinformation that slips through. However, it is important to acknowledge that implementing a better defense system could also accidentally delete a real post. This accident would likely trigger further distrust in democracy and media, only making the situation worse, so more thought is needed to carefully form a response plan.

Conclusion

Although increased monitoring raises valid concerns about individual privacy, action must still be taken to counter Russian disinformation campaigns. These campaigns threaten U.S. national sovereignty by exploiting personal beliefs, media ecosystems, and social divisions to erode public faith in democracy. They also aim to manipulate elections and foreign

[37] Ibid., 27

[38] Ibid.

policy, ultimately weakening the United States and its commitment to democratic alliances. NATO — the cornerstone of mutual defense among democracies — is a primary target because it obstructs Putin's expansionist goals and challenges his regime simply by existing.

To effectively counter Russian disinformation, the United States must strengthen coordination with media and tech companies, grassroots organizations, NATO, and other democracies. Ongoing analysis of Russian capability development should be shared with the systems — both human and AI — tasked with monitoring and defending the information space. Just as crucial is a dramatic expansion of public awareness campaigns to educate Americans on the nature of foreign malign influence, the threat it poses, and how to recognize it in action.

There also needs to be more research on this topic. My research relies on publicly available government reports, but national security reports do not reveal the full extent of covert operations by nature. This censorship provides an obstacle for academic analysis. Research relying on private investigation and studies may help to further explore this subject. I also sincerely urge the reader to view my sources for themselves, interpret them, think about how to respond, and educate others on the threat, tactics, and needed responses to Russian and other foreign disinformation campaigns.

Bibliography

Bergmanis-Korāts, G., Isupova, M., Vecmanis, R. R. "Virtual Manipulation Brief 2025: From War and Fear to Confusion and Uncertainty." Riga: NATO Strategic Communications Centre of Excellence.

Conley, Heather A., "Undermining Democracy: Kremlin Tools of Malign Political Influence." Center for Strategic and International Studies (CSIS), 2019. http://www.jstor.org/stable/resrep37610.

Defence Technical Information Center. Robert J. Moschella, Lt Col, USAF. *The Besieged Fortress: Making Sense of Russia's Annexation of Crimea and What It Means to U.S. Policy Makers.* Accessed August 5, 2025. https://apps.dtic.mil/sti/citations/AD1038278.

Diuk, Nadia. "Euromaidan: Ukraine's Self-Organizing Revolution." *World Affairs* 176, no. 6 (2014): 9–16. http://www.jstor.org/stable/43555086.

Federal Bureau of Investigation. "Russian Interference in 2016 U.S. Elections." Accessed June 19, 2025. https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections.

Filipova, Rumena, Bart Hogeveen, Ivana Karásková, Patryk Pawlak, and Andrea Salvi. "The Kremlin's Agenda in Bulgaria: The Role of Pro-Neutrality Protests in Disinformation Campaigns." Edited by Nad'a Kovalčíková. In *Hacking Minds and Machines: Foreign Interference in the Digital Era*. European Union Institute for Security Studies (EUISS), 2024. http://www.jstor.org/stable/resrep62147.5.

Moskowitz, Ken. "Did NATO Expansion Really Cause Putin's Invasion? A Seasoned Diplomat Considers This Question in Light of His Own Experience." *Foreign Service Journal*, October 2022. Accessed August 5, 2025. https://afsa.org/did-nato-expansion-really-cause-putins-invasion.

Nakayama, Bryan. "Democracies and the Future of Offensive (Cyber-Enabled) Information Operations." *The Cyber Defense Review* 7, no. 3 (2022): 49–66. https://www.jstor.org/stable/48682322.

National Intelligence Council. "Foreign Threats to the 2020 U.S. Federal Elections." Accessed June 19, 2025. https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf.

NATO Review. "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote." Accessed August 5, 2025. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html.

Robbins, Joseph W., Heather A. Conley, Robert Person, Jim Golby, Gil Barndollar, and Jade McGlynn. "Countering Russian Disinformation." Edited by Mark F. Cancian and Cyrus Newlin. In *The Diversity of Russia's Military Power: Five Perspectives*. Center for Strategic and International Studies (CSIS), 2020. http://www.jstor.org/stable/resrep26533.8.

Salvi, Andrea, Rumena Filipova, Bart Hogeveen, Ivana Karásková, and Patryk Pawlak. "The Attack of the Clones: Deepfakes and the Evolving Landscape of Disinformation." Edited by Nad'a Kovalčíková. In *Hacking Minds and Machines: Foreign Interference in the Digital Era*. European Union Institute for Security Studies (EUISS), 2024. http://www.jstor.org/stable/resrep62147.7.

U.S. Cyber Command. "Russian Disinformation Campaign 'DoppelGänger' Unmasked: A Web of Deception." Accessed June 16, 2025. https://www.

cybercom.mil/Media/News/Article/3895345/russian-disinformation-campaign-doppelgnger-unmasked-a-web-of-deception.

U.S. Department of Justice. "Guerilla Media Campaign in the United States." Accessed June 20, 2025. https://www.justice.gov/archives/opa/media/1366196/dl.

U.S. Department of Justice. "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere." Accessed June 16, 2025. https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence.

U.S. Department of Justice. "The Good Ole USA ('Good Ole USA') Project." Accessed June 20, 2025. https://www.justice.gov/archives/opa/media/1366201/dl.

U.S. Department of Justice. "US Social Media Influencers Network." Accessed June 20, 2025. https://www.justice.gov/archives/opa/media/1366191/dl.

U.S. Department of State. "Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War." Accessed August 5, 2025. https://2021-2025.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war.

U.S. Government Accountability Office. "Foreign Disinformation: Defining and Detecting Threats." Accessed June 27, 2025. https://www.gao.gov/assets/gao-24-107600.pdf.

Vázquez Liñán, Miguel. "History as a Propaganda Tool in Putin's Russia." *Communist and Post-Communist Studies* 43, no. 2 (2010): 167–78. https://www.jstor.org/stable/48609753.

2

Conflict and Contagion: Addressing the Nexus of Sociopolitical Instability and Health Security in WHO's Health Emergency Frameworks

Tanvi MERIANDA

Abstract: In today's age of asymmetric warfare and hybrid threats, health security in sociopolitically unstable contexts faces unprecedented challenges. Conflicts and political instability disrupt healthcare infrastructure, complicate disease surveillance, and hinder effective emergency responses. Such complex environments require adaptable, context-aware health systems capable of navigating shifting power dynamics and fragmented governance. This research examines how WHO's health emergency frameworks perform in such settings, focusing on improvements in surveillance, alert + response, and operations. It highlights the urgent need to incorporate political realities and flexible governance to enhance preparedness and response in fragile environments.

Keywords: World Health Organization, Health Security, Hybrid Threats, Sociopolitical Instability, Humanitarian Emergencies

Introduction

In an era defined by overlapping crises, the targeting of healthcare systems by violent non-state actors marks a profound shift in the nature of modern conflict. Frank Hoffman's hybrid threats theory offers a useful lens for understanding this shift, emphasizing that epidemics do not occur in isolation but intersect with illicit economies, digital warfare, and fragmented governance.[39] Hybrid threats involve the coordinated use of both conventional and unconventional tactics — including terrorism, cyberattacks, disinformation, and infrastructure sabotage — by state or non-state actors to destabilize societies and achieve political objectives.[40] Health systems, particularly in fragile states, have increasingly become tools and targets in these campaigns. According to recent data, "Over the course of 5 years, 1,721 healthcare facilities were damaged, 2,153 healthcare personnel were injured, and 485 patients were harmed in these attacks."[41] When viewed through the lens of asymmetric warfare, these attacks are not random acts of violence, but strategic efforts by less-resourced groups to exploit health vulnerabilities, undermine public trust, and exert influence without engaging in direct military confrontation.

The bidirectional nexus between sociopolitical violence and the functionality of healthcare can be understood by applying the hybrid threats framework to global health security operations. Sociopolitical violence is defined in this paper as acts of aggression, coercion, or disruption arising from or directed toward political, ethnic, or religious structures, and encompasses a wide array of conflict modalities — including terrorism, civil insurgency, and state-sponsored repression.[42] The relationship between violence and health insecurity is cyclical; conflict weakens healthcare capacity, while

---

[39] Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, VA: Potomac Institute for Policy Studies, 2007), https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

[40] Ibid.

[41] Fatih Cemal Tekin and Fatma Selcen Ocal, "Attacks on Health Care Worldwide: 5-Year Review," *Eurasian Journal of Emergency Medicine* 22, no. 4 (2023): 211–16, https://doi.org/10.4274/eajem.galenos.2023.42223.

[42] Jeff Hearn et al., "Violence Regimes: A Useful Concept for Social Politics, Social Analysis, and Social Theory," *Theory and Society* 51 (2022), https://doi.org/10.1007/s11186-022-09474-4.

deteriorating health systems intensify grievances and destabilization. Yet, health systems are not merely passive victims of instability — they can also serve as critical stabilizing forces. In contexts where state institutions are weak or absent, the presence of reliable health infrastructure can fill governance vacuums, restore public trust, and reduce incentives for political violence.[43] This research focuses on the World Health Organization (WHO), whose emergency preparedness architecture — including its surveillance, alert and response, and operations frameworks — plays a pivotal role in conflict-sensitive health interventions. Through a case study of WHO's polio eradication efforts in Pakistan, this paper explores how the organization can more effectively integrate the risks posed by sociopolitical violence into its health security mandate. By doing so, WHO can enhance resilience in complex humanitarian emergencies and improve the efficacy of its interventions in politically volatile settings.

Operationalizing the WHO

Founded on April 7th, 1948, the WHO is an intergovernmental body within the United Nations system that specializes in addressing global public health crises and advancing health equity. Central to WHO's work is its role in global health security, as it monitors disease outbreaks, facilitates rapid data sharing, and supports preparedness efforts that mitigate cross-border threats. WHO's efforts not only protect population health but also contribute to broader sociopolitical stability by ensuring that health emergencies do not escalate into political or economic crises.

Woven within the practices of WHO is the framework laid out by the 2005 International Health Regulations (IHR) authorizing the organization to serve as the main hub for all essential disease surveillance information.[44] As stated in the official WHO website, "WHO plays the coordinating role

[43] Yazan Douedari and Natasha Howard, "Perspectives on Rebuilding Health System Governance in Opposition-Controlled Syria: A Qualitative Study," *International Journal of Health Policy and Management* 8, no. 4 (2019): 233–44, https://doi.org/10.15171/ijhpm.2018.132.

[44] Jeremy Youde, "The International Health Regulations," *Biopolitical Surveillance and Public Health in International Politics*, 2010, 147–75, https://doi.org/10.1057/9780230104785_7.

in IHR implementation and […] helps countries to build capacities."[45] This responsibility is reflected in its emergency framework: surveillance (early threat detection), alert and response (rapid coordination), and operations (on-the-ground support and recovery). These pillars will serve as the framework through which I contextualize the scope and impact of an organization as extensive as the WHO.

Surveillance

The WHO defines public health surveillance as the "continuous, systematic collection and analysis of health-related data to guide public health planning and response" — crucial during emergencies for timely detection and coordination.[46] Effective surveillance must include not just clinical indicators but also sociopolitical factors like conflict intensity, community trust, and social disruption. One key WHO mechanism addressing these is the Surveillance System of Attacks on Healthcare (SSA), which tracks assaults on medical services in conflict zones. By contextualizing warfare and managing tactical data, SSA supports trend analysis in unstable regions. However, its limited granularity — such as missing geocoding, impact metrics, and intent indicators — hinders understanding of health insecurity and weakens emergency response.[47]

Moreover, trust in the SSA remains low among frontline health actors, especially in conflict zones like Syria and Ethiopia, where the system's reliance on self-reporting through NGOs and mobile applications has seen limited adoption[48]. In regions such as Northwest Syria, the SSA is not in use at all,

---

[45] World Health Organization, "International Health Regulations," *WHO.int*, last modified 2024, https://www.who.int/health-topics/international-health-regulations.

[46] World Health Organization, "Surveillance in Emergencies," World Health Organization, 2023, https://www.who.int/emergencies/surveillance.

[47] Benjamin Mason Meier, Hannah Rice, and Shashika Bandara, "Monitoring Attacks on Health Care as a Basis to Facilitate Accountability for Human Rights Violations," *Health and Human Rights* 23, no. 1 (June 2021): 55, https://pmc.ncbi.nlm.nih.gov/articles/PMC8233025.

[48] Reem Ladadwa et al., "Health Information Management Systems and Practices in Conflict-Affected Settings: The Case of Northwest Syria," *Globalization and Health* 20, no. 1 (June 6, 2024), https://doi.org/10.1186/s12992-024-01052-w.

with health workers citing issues around usability, inadequate protection mechanisms for reporters, and security concerns that deter engagement.[49] This disconnect between the SSA's centralized structure and the complex realities of health workers operating under threat contributes to underreporting and widespread skepticism about the system's effectiveness. While the SSA provides a framework for tracking violence against healthcare, its low granularity and lack of trust limit its use for proactive, context-aware interventions — reducing it to a reactive reporting tool.

While the SSA reflects WHO's attempt to document violence against healthcare, the Health Emergency Preparedness, Response and Resilience (HEPR) framework takes a more holistic approach by embedding sociopolitical awareness into emergency preparedness systems, particularly in fragile and conflict-affected settings. Recognizing that "one size does not fit all," HEPR strengthens resilience by linking surveillance with community protection and coordination across multiple stakeholders, especially where state systems are weak or absent[50]. It promotes triangulating diverse data sources, such as NGO reports, local observations, and market signals, to detect threats early and compensate for unreliable government reporting. HEPR emphasizes adaptability and real-time responsiveness by using field-generated evidence to continuously refine crisis strategies, while promoting horizontal and vertical integration to coordinate across sectors and address local governance gaps, distrust, and intersecting vulnerabilities. By supporting decentralized decision-making such as United Nations Relief and Works Agency's successful delegation to field offices during the Syrian refugee crisis, HEPR enhances public health system flexibility and aligns emergency response with broader peacebuilding and development objectives.[51]

---

[49] Ibid.

[50] World Health Organization, *10 Proposals to Build a Safer World Together: Strengthening the Global Architecture for Health Emergency Preparedness, Response and Resilience* (Geneva: World Health Organization, 2022), https://cdn.who.int/media/docs/default-source/emergency-preparedness/who_hepr_june30draftforconsult.pdf.

[51] Lena Forsgren et al., "Health Systems Resilience in Practice: A Scoping Review to Identify Strategies for Building Resilience," *BMC Health Services Research* 22, no. 1 (September 19, 2022), https://doi.org/10.1186/s12913-022-08544-8.

While HEPR promotes collaborative surveillance across sectors, it appears to lack explicit mechanisms for integrating political dynamics such as shifts in territorial control, cease-fire status, or fluctuations in community trust into its risk monitoring framework. Conflict-sensitive surveillance in volatile settings such as the Eastern Democratic Republic of the Congo illustrates that conflict not only disrupts healthcare infrastructure, but also erodes community trust and skews healthcare-seeking behavior — factors which routine surveillance frameworks, including HEPR, are ill-equipped to detect.[52] Without embedding these political risk signals, HEPR's monitoring runs the risk of being blind to early warning signs that precede governance breakdowns or health system collapse in fragile contexts.

Alert and Response

Under the IHR, WHO supports national responses and facilitates global information-sharing to prevent cross-border spread. Two major tools in this effort are the Electronic Early Warning, Alert, and Response System (EWARS), which accelerates outbreak detection via digital platforms, and the Health Emergency and Disaster Risk Management Framework (Health-EDRM), which offers a multisectoral approach to crisis management. While effective in stable emergency contexts, both frameworks face significant limitations in conflict zones characterized by sociopolitical violence and weak governance.

EWARS is a digital surveillance tool designed for rapid deployment in crisis-affected, low-resource settings, operating through mobile platforms to detect disease outbreaks via a built-in risk matrix and real-time alert system. Delivered as a self-contained kit with mobile devices, solar chargers, and a local server, it functions independently of local infrastructure and has proven effective in emergency settings with urgent health needs. During the Rohingya refugee crisis in Bangladesh, it provided real-time

[52] Olivier Kambere Kavulikirwa, "Intersecting Realities: Exploring the Nexus between Armed Conflicts in Eastern Democratic Republic of the Congo and Global Health," *One Health* 19 (December 1, 2024): 100849–49, https://doi.org/10.1016/j.onehlt.2024.100849.

data that informed measles vaccination efforts and Hepatitis A prevention responses, highlighting EWARS' strength as a scalable, digital innovation that enhances disease surveillance and response in crisis zones.[53] Yet EWARS struggles in conflict zones shaped by asymmetric warfare and sociopolitical violence. In regions like Northwest Syria, constant displacement and the collapse of public institutions undermine the system's ability to maintain reliable data flows.[54] The 2015 data void for Idlib governorate — coinciding with regime withdrawal and non-state group control — exposed its dependence on functioning governance.[55] Without integrating local capacity and sociopolitical dynamics, global health frameworks risk reinforcing the very governance vacuums they aim to mitigate.

Building on EWARS' limitations, the Health-EDRM is WHO's broader attempt to integrate sociopolitical and structural vulnerabilities into emergency planning. Established in 2019, it promotes a risk-based, all-hazards approach that prioritizes prevention, preparedness, response, and recovery within health systems[56]. While designed to align with strategies like UHC, the IHR, the Sendai Framework, and climate action, its implementation in conflict-affected regions still reveals major gaps in political adaptability and operational feasibility. An illustrative example is the postpartum hemorrhage prevention project deployed across ten conflict-prone provinces of Afghanistan[57]. This effort prioritized

---

[53] Basel Karo et al., "World Health Organization Early Warning, Alert and Response System in the Rohingya Crisis, Bangladesh, 2017–2018," *Emerging Infectious Diseases* 24, no. 11 (2018): 2074–76, https://doi.org/10.3201/eid2411.181237.

[54] Reem Ladadwa et al., "Health Information Management Systems and Practices in Conflict-Affected Settings: The Case of Northwest Syria," *Globalization and Health* 20, no. 1 (2024), https://doi.org/10.1186/s12992-024-01052-w.

[55] Annie Sparrow et al., "Cholera in the Time of War: Implications of Weak Surveillance in Syria for the WHO's Preparedness—a Comparison of Two Monitoring Systems," *BMJ Global Health* 1, no. 3 (October 2016): e000029, https://doi.org/10.1136/bmjgh-2016-000029.

[56] "World Health Organization, *Health Emergency and Disaster Risk Management Framework* (Geneva: World Health Organization, 2019), https://iris.who.int/bitstream/handle/10665/326106/9789241516181-eng.pdf?sequence=1.

[57] Gopireddy Murali et al., "Action Plan Open Access Digitally Strengthened, Midwife-Led Intervention to Reach the Unreached Mothers across Ten Conflict-Prone Provinces of Afghanistan during Humanitarian Crisis," *Nursing and Midwifery Studies* 12, no. 2 (2023), https://doi.org/10.48307/NMS.2023.175273.

coordination with community and religious leaders to achieve its goal of expanding maternal health access in remote areas during crisis conditions[58]. This approach stands in contrast to other WHO tools, such as EWARS in Northwest Syria, where lack of local participation and top-down structure undermined implementation in volatile zones. Despite its flexible design, Health-EDRM struggles in complex conflict settings like Balochistan, where Afghan refugee populations and fractured governance pose major challenges. Political tensions with the central government have led to chronic underdevelopment and neglect of basic services, including healthcare.[59] Without clear guidance on how to implement health interventions when the state is a party to the conflict, the Health-EDRM framework risks becoming aspirational rather than operational in its most critical settings.

Operations

As previously discussed in terms of surveillance and alert + response, sociopolitical instability and hybrid threats undermine not only preparation for emergent health crises but also the operational delivery of health interventions. Both the WHO's Incident Management System (IMS) and National Action Plan for Health Security (NAPHS) are essential mechanisms that aim to operationalize the IHR, but they too are challenged in fragile and non-permissive settings. "Operations" in WHO frameworks requires secure coordination, clear authority, and flexible decision-making — conditions often absent in asymmetric warfare contexts.

The IMS is WHO's standardized but flexible operational architecture for coordinating national and international actors under a single chain of command during health emergencies. Scalable and hierarchical, IMS enhances resource deployment and technical support while adapting to the size and

[58] Ibid.

[59] Yasir Shafiq et al., "Toward Resilient Maternal, Neonatal and Child Health Care: A Qualitative Study Involving Afghan Refugee Women in Pakistan," *Health Services Insights* 18 (2025), https://doi.org/10.1177/11786329241310733.

complexity of a crisis.[60] Beyond technical coordination, IMS has strategic relevance in politically unstable contexts shaped by hybrid threats, where it functions not only as a public health tool but as a stabilizing mechanism in environments threatened by insurgents, paramilitary actors, or disinformation campaigns. During the 2014–2016 Ebola outbreak, WHO and national governments used IMS-enabled Emergency Operations Centers in Liberia, Sierra Leone, and Guinea to tailor response coordination to local political realities.[61] This modular approach allowed for cooperation with subnational structures and, when necessary, non-state actors — preserving data flow and care continuity amid asymmetric conflict. Similarly, during Nigeria's 2019 Lassa Fever outbreak, the One Health IMS model integrated actors across health, agriculture, and environment ministries.[62] Even in conflict-affected states like Taraba and Adamawa, the Nigeria Field Epidemiology Training Program mobilized locally trained responders to deliver case management and surveillance, demonstrating that IMS can function in contested spaces when supported by national leadership and workforce development.

Yet despite its adaptability, IMS remains constrained by assumptions of centralized authority and institutional trust — conditions rarely met in hybrid warfare settings, where misinformation is weaponized and low public trust renders its reliance on coordination and standardization a liability. While adaptations like One Health offer promise, they depend on political will, multisectoral buy-in, and strong ministries — elements often missing in conflict zones.[63] Without embedding political

---

[60] World Health Organization, *ERF Emergency Response Framework: Internal WHO Procedures* (Geneva: World Health Organization, 2024), https://iris.who.int/bitstream/handle/10665/375964/9789240058064-eng.pdf?sequence=1.

[61] Jennifer C. Brooks et al., "Incident Management Systems and Building Emergency Management Capacity during the 2014–2016 Ebola Epidemic — Liberia, Sierra Leone, and Guinea," *MMWR Supplements* 65, no. 3 (July 8, 2016): 28–34, https://doi.org/10.15585/mmwr.su6503a5.

[62] Chioma Dan Nwafor et al., "The One Health Approach to Incident Management of the 2019 Lassa Fever Outbreak Response in Nigeria," *One Health* 13 (December 2021): 100346, https://doi.org/10.1016/j.onehlt.2021.100346.

[63] Richard Brennan, Rana Hajjeh, and Ahmed Al-Mandhari, "Responding to Health Emergencies in the Eastern Mediterranean Region in Times of Conflict," *The Lancet* 399, no. 10332 (March 2020), https://doi.org/10.1016/s0140-6736(20)30069-6.

intelligence, community trust-building, and flexible engagement strategies into its design, IMS risks failure in precisely the fragile environments it aims to stabilize.

Unlike the IMS, which is designed for acute response, NAPHS is a long-term preparedness tool aligned with the IHR, offering a systemic, comprehensive approach to public health emergencies. While not initially designed for conflict settings, its multisectoral and long-term architecture makes it particularly promising for addressing hybrid threats in sociopolitically unstable environments when properly adapted. NAPHS promotes inclusive, evidence-based health security by integrating sectors like defense, agriculture, finance, and civil society, fostering national ownership and attracting donor support through alignment with Joint External Evaluation assessments. In lower-income or post-conflict settings, this multisectoral model can mitigate institutional fragmentation, build trust between central and local actors, and strengthen the social contract when grounded in transparency and local engagement.[64]

However, NAPHS' success depends on baseline political cohesion and coordination capacity — conditions often absent in fragile or conflict-affected states. In cases like Ethiopia, regional conflict and waning political commitment have disrupted even well-documented NAPHS efforts, revealing the plan's vulnerability to instability. When applied uniformly without adapting to sociopolitical fault lines — such as mistrust in institutions, the presence of non-state actors, or asymmetric warfare — NAPHS risks becoming a top-down intervention that reinforces inequities rather than builds resilience. To remain effective in such contexts, NAPHS must be context-specific, and rooted in local stakeholders to avoid exacerbating the very fragilities it seeks to address.

[64] Charles Njuguna et al., "Improving Global Health Security through Implementation of the National Action Plan for Health Security in Sierra Leone, 2018–2021: Lessons from the Field," *BMC Public Health* 23, no. 2178 (November 7, 2023), https://doi.org/10.1186/s12889-023-17103-7.

Case Study: The Polio Eradication Crisis in Pakistan

Figure 1: Map of Pakistan's provinces before the dissolution of the Federally Administered Tribal Areas

Source: Orris, Greta J., Pamela Dunlap, John Wallis, and Jeff Wynn. "Phosphate Occurrence and Potential in the Region of Afghanistan, Including Parts of China, Iran, Pakistan, Tajikistan, Turkmenistan, and Uzbekistan." *Open-File Report*, 2015. https://doi.org/10.3133/ofr20151121.

Poliomyelitis, or polio, is a highly contagious disease that thrives in conditions of poor sanitation; requiring sustained, widespread immunization to prevent outbreaks. This virus is particularly vulnerable to sociopolitical disruptions that hinder vaccination and surveillance. While the Global Polio Eradication Initiative (GPEI) has made significant progress since 1988, Pakistan — alongside Afghanistan — remains one of only two countries where wild poliovirus remains endemic.[65] Despite extensive vaccination

[65] Pakistan Polio Eradication Programme, "Eradication Strategy," *End Polio Pakistan*, accessed July 30, 2025, https://www.endpolio.com.pk/polioin-pakistan/eradication-strategy.

campaigns, progress has been impeded by deep-rooted political instability, chronic underinvestment in public health, and a lack of trust between marginalized communities and the state. In rural areas, where basic services like clean water and electricity are absent, vaccination drives are often viewed as misplaced priorities, deepening the disconnect between public health initiatives and broader development needs.[66]

Militancy, ideological propaganda, and sociopolitical fragmentation have further entrenched the crisis, turning a public health issue into a complex security challenge. In 2006–2007, Tehrik-i-Taliban Pakistan (TTP) affiliate Maulana Fazlullah weaponized religious rhetoric via FM radio in Malakand, labeling polio vaccines as haram and part of a Western sterilization plot. The misinformation endured into the 2010s, leading to approximately 150,000 families having denied the polio vaccination.[67] These conspiracies gained traction, especially after the 2011 CIA operation in Abbottabad, which used a fake Hepatitis B campaign to gather DNA for the Osama bin Laden raid.[68] Such state interference exemplifies Foucault's theory of biopolitics, where health is used as a tool for population control, leading to an erosion of trust in government authorities.[69] As this trust deteriorated, immunization efforts were increasingly viewed not as care, but as surveillance and coercion, heightening skepticism toward both the Pakistani state and international health actors.

The aftermath has been deadly and destabilizing. Polio workers have become frequent targets: in 2012, eight vaccinators were assassinated across several cities; in 2015, others were kidnapped and killed in Balochistan; and in 2025, a police officer was murdered while guarding

---

[66] Pakistan Polio Eradication Programme, "Eradication Strategy.

[67] Sumaira Kanwal et al., "Regression in Polio Eradication in Pakistan: A National Tragedy," *Journal of the Pakistan Medical Association* 66, no. 3 (March 3, 2016): 328–33, https://www.researchgate.net/publication/297715432_Regression_in_polio_eradication_in_Pakistan_A_national_tragedy#.

[68] Shahella Idrees Shakeel et al., "Achieving the End Game: Employing 'Vaccine Diplomacy' to Eradicate Polio in Pakistan," *BMC Public Health* 19, no. 1 (January 17, 2019), https://doi.org/10.1186/s12889-019-6393-1.

[69] Btihaj Ajana, "Surveillance and Biopolitics," *Electronic Journal of Sociology* 7 (2025), https://kclpure.kcl.ac.uk/portal/en/publications/surveillance-and-biopolitics.

vaccinators in Noshki.[70] From 2012 to 2014, militants banned polio vaccines in North Waziristan, citing U.S. drone strikes as justification. These bans and attacks reveal the extent of political fragmentation, especially in regions like the former Federally Administered Tribal Areas (FATA), where non-state actors often held more power than the federal government. Such local non-state actors have prevented more than 350,000 children from being vaccinated for polio since June 2012.[71] Grassroots resistance has also emerged in less violent forms: in 2019, Parachinar residents boycotted polio campaigns to protest neglected infrastructure and religious sites. A similar trend was seen throughout the FATA where 59% of the population stated they would rather prioritize clean water over polio eradication around 66% stated that energy/fuel issues should take precedence.[72] Such rebellion aligns with Scott's Theory of Everyday Resistance where, for these communities, refusing vaccination becomes a symbolic assertion of autonomy and a critique of a state that delivers syringes while failing to provide clean water or safe schools.[73]

Ultimately, the polio crisis in Pakistan illustrates how sociopolitical instability actively undermines public health systems, functioning as a form of hybrid threats by non-state actors. Militant groups like the TTP have deliberately targeted healthcare infrastructure to weaken state authority, using misinformation campaigns and violent attacks to erode trust in both the government and international health institutions. The assassination of vaccinators, bans on immunization, and the use of religious rhetoric to delegitimize vaccines transform what should be a neutral

---

[70] Braira Wahid et al., "The History and Current Killings of Polio Vaccinators in Pakistan: A Need for Targeted Surveillance Strategy," *Asia-Pacific Journal of Public Health*, March 1, 2023, 101053952311588-101053952311588, https://doi.org/10.1177/10105395231158866.

[71] Edna K Moturi et al., "Progress toward Polio Eradication — Worldwide, 2013–2014," *Morbidity and Mortality Weekly Report* 63, no. 21 (May 30, 2014): 468, https://pmc.ncbi.nlm.nih.gov/articles/PMC5779464.

[72] Gillian K. SteelFisher et al., "Threats to Polio Eradication in High-Conflict Areas in Pakistan and Nigeria: A Polling Study of Caregivers of Children Younger than 5 Years," *The Lancet Infectious Diseases* 15, no. 10 (October 2015): 1183–92, https://doi.org/10.1016/s1473-3099(15)00178-4.

[73] Richard Ballard, "Everyday Resistance," in *The Routledge Handbook of Social Change*, ed. Richard Ballard and Clive Barnett (London: Routledge, 2022), 303–14, https://doi.org/10.4324/9781351261562-29.

public health initiative into a contested ideological battleground. Acts of violence and propaganda, while not traditional warfare, strategically destabilize state legitimacy by making the government appear incapable of delivering even basic services. In this context, health infrastructure becomes a proxy for political control, and its disruption serves to amplify governance failures. Weaponizing public health aligns with the logic of asymmetric warfare, where weaker non-state actors exploit vulnerabilities such as dependency on international aid or public distrust to counter more powerful state actors. The result is a cycle of fragility: poor health outcomes reinforce sociopolitical unrest, which in turn further debilitates health systems. As grassroots resistance grows — whether through boycotts, misinformation, or outright violence — the failure of international health organizations like the WHO to address the underlying structural inequities only entrenches this cycle. Thus, Pakistan's enduring polio endemic is not simply a failure of immunization, but a symptom of a broader political struggle in which healthcare itself becomes a site of conflict and fragmentation.

WHO Intervention in Pakistan

One of the WHO's most effective strategies in tackling Pakistan's hybrid polio crisis has been vaccine diplomacy through community integration. Aware of the mistrust many communities harbored — exacerbated by extremist propaganda portraying vaccines as Western tools for sterilization — the WHO collaborated with local religious leaders, and tribal elders to deliver health education grounded in cultural and religious values.[74] This bottom-up approach succeeded in increasing vaccine acceptance in historically resistant regions, illustrating the power of community-rooted partnerships in shifting public perception and building sustainable trust in health interventions.

[74] Shahella Idrees Shakeel et al., "Achieving the End Game: Employing 'Vaccine Diplomacy' to Eradicate Polio in Pakistan," *BMC Public Health* 19, no. 1 (January 17, 2019), https://doi.org/10.1186/s12889-019-6393-1.

However, these gains remain fragile in the face of deep-rooted educational inequities, particularly in conflict-affected areas like the former FATA. Years of violence have devastated infrastructure — over 360 schools were destroyed in 2015 alone — leading to an overall literacy rate of just 28.4%.[75] A lack of education reduces health literacy, making communities more vulnerable to misinformation and less likely to participate in vaccination campaigns. In this context, poor literacy is both a consequence and a driver of insecurity, as weakened health systems struggle to contain outbreaks that, in turn, perpetuate sociopolitical instability. For WHO strategies to be truly effective, they must address this intersection of conflict, education, and public health, recognizing that vaccine delivery alone cannot solve systemic vulnerabilities.

The GPEI, launched in 1988, has been central to coordinating global efforts, deploying mass immunization campaigns, surveillance networks, and cross-border cooperation with Afghanistan[76]. In Pakistan, the initiative has mobilized thousands of vaccinators and surveillance officers in alignment with WHO's NAPHS. Yet despite these intensive efforts, wild poliovirus remains endemic in Pakistan — a sign of the limitations of top-down, vertical health interventions. Critics like anthropologist Sara Closser have pointed out that the focus on rapid eradication has often overshadowed long-term development, such as improving sanitation or funding routine immunization services.[77] Only 10% of Pakistan's health budget is allocated to primary healthcare, while the independently managed polio eradication program receives full financial coverage — creating a stark imbalance in visible government priorities. Feelings of neglect fuel resentment in underserved areas like former FATA and Balochistan, where communities grappling with high infant mortality from preventable diseases such as diarrhea often view polio campaigns as irrelevant, leaving room for local

[75] Ibid.

[76] Shazia Ghafoor and Nadeem Sheikh, "Eradication and Current Status of Poliomyelitis in Pakistan: Ground Realities," *Journal of Immunology Research* 2016 (2016): 1–6, https://doi.org/10.1155/2016/6837824.

[77] Svea Closser, "Why Eradicating Polio Is More Complicated than It Seems," *SAPIENS*, July 11, 2018, https://www.sapiens.org/culture/polio-eradication-pakistan.

actors and militants to exploit these sentiments and deepen mistrust in state leadership.[78]

To eradicate polio in Pakistan, the WHO must recalibrate its approach to account for the sociopolitical dynamics that undermine public health. In areas destabilized by militancy and mistrust, partnering with local leaders and culturally credible actors is essential to protect vaccinators and rebuild legitimacy. Combating propaganda requires not just health messaging, but long-term investment in education — especially in conflict zones where low literacy fuels misinformation. Above all, healthcare must be integrated into broader development efforts that deliver visible benefits like clean water and maternal care. When communities feel their basic needs are ignored, health campaigns appear coercive rather than caring. By embedding immunization within a framework of trust-building, infrastructure, and responsive governance, the WHO can transform polio eradication from a contested intervention into a collaborative, community-driven success.

Constraints and Considerations

A core limitation of WHO's work in conflict zones is its institutional commitment to political neutrality. In volatile regions where foreign agendas are met with suspicion, the WHO's perceived neutrality is often the only reason it can operate at all. However, avoiding political critique creates a strategic paradox: without naming the militant or political actors — such as extremist groups spreading vaccine misinformation or attacking health workers — the WHO struggles to fully address barriers to healthcare access. This delicate balancing act between diplomacy and security impairs the organization's ability to implement comprehensive health strategies in politically charged environments.

Additionally, the increasing securitization of health by global actors like the WHO introduces both operational and ethical implications. Framing health

[78] Aurangzaib Khan, "Polio: What's behind the Refusals?," DAWN.COM, September 29, 2019, https://www.dawn.com/news/1507831.

through a security lens can lead to prioritizing diseases that pose a global threat over those causing chronic, localized suffering. This dynamic may divert resources from essential health services toward emergency responses, thereby reinforcing global health inequities. Communities may begin to question whether the WHO's intent is to promote health for all or to protect certain populations from the spillover effects of disease. This erosion of trust can be particularly dangerous in contexts where misinformation is already rampant. Furthermore, no framework — no matter how robust or evidence-based — can fully account for the instability, fragmentation, and fast-changing nature of conflict zones. From sudden displacement and collapsing infrastructure to the rise of new militant actors, conditions on the ground often shift faster than any institution can respond, demanding constant reassessment and humility in the face of uncertainty.

Policy Recommendation

Health interventions must be leveraged as immediate responses to crises and as strategic tools to strengthen local stability and resilience against complex hybrid threats. Standardized global strategies frequently overlook the complex sociocultural and historical dynamics of local communities, treating them as homogenous targets rather than diverse, lived realities. The WHO should prioritize context-specific approaches informed by deep, localized understanding rather than narrowly focusing on rapid eradication efforts alone. The polio crisis in Pakistan demonstrated how this rush toward quick fixes often overshadows sustainable, long-term development initiatives, such as improving social inequalities, which are essential for durable health security.

By embedding interventions within the socio-political realities of affected regions, the WHO can become more proactive and adaptive in facing hybrid threats, including those posed by non-state actors who exploit health vulnerabilities to undermine governance and social cohesion. These actors increasingly dismantle community trust in foreign interventions, eroding the necessary foundation for capacity building. Therefore, building long-term trust within communities, perhaps by increasing local ownership

amid NAPHS-led capacity building, must become a core priority for the WHO. Without sustained trust, efforts to enhance health systems and governance will face persistent resistance and diminished effectiveness. Only through genuine partnerships, respect for local knowledge, and consistent engagement can health interventions contribute to lasting peace, stability, and resilience in fragile settings.

Conclusion

The evolving challenges faced by fragile and conflict-affected regions demand a fundamental shift in how global health interventions are designed and implemented. As non-state actors increasingly exploit local instability and erode trust in foreign involvement, traditional short-term emergency responses are no longer sufficient. Without sustained efforts to build trust and deepen understanding of local contexts, interventions risk further alienating communities and undermining long-term capacity building. The WHO and other international organizations must therefore prioritize context-specific strategies that incorporate political, social, and cultural dynamics to effectively address hybrid threats and support local resilience.

Given the vast scope of the WHO's initiatives and the diverse sociopolitical landscapes in which it operates, further research is essential to understand how different contexts influence the effectiveness of health interventions. Comparative studies across various regions affected by conflict and instability could provide valuable insights into how local dynamics shape outcomes. Such inquiry will be crucial to refining strategies that promote sustainable health improvements while mitigating political and security risks in fragile environments.

This moment represents a critical opportunity to rethink global health diplomacy — not only as a tool for immediate crisis management but as a foundation for durable peace and stability. Only by grounding interventions in the lived realities of communities and committing to sustained, long-term partnership can we rebuild trust and shape the lasting empowerment that fragile regions so desperately need.

Bibliography

Ajana, Btihaj. "Surveillance and Biopolitics." *Electronic Journal of Sociology* 7 (2025). https://kclpure.kcl.ac.uk/portal/en/publications/surveillance-and-biopolitics.

Ballard, Richard. "Everyday Resistance." In *The Routledge Handbook of Social Change*, edited by Richard Ballard and Clive Barnett, 303–14. London: Routledge, 2022. https://doi.org/10.4324/9781351261562-29.

Brennan, Richard, Rana Hajjeh, and Ahmed Al-Mandhari. "Responding to Health Emergencies in the Eastern Mediterranean Region in Times of Conflict." *The Lancet* 399, no. 10332 (March 2020). https://doi.org/10.1016/s0140-6736(20)30069-6.

Brooks, Jennifer C., Meredith Pinto, Adrienne Gill, Katherine E. Hills, Shivani Murthy, Michelle N. Podgornik, Luis F. Hernandez, Dale A. Rose, Frederick J. Angulo, and Peter Rzeszotarski. "Incident Management Systems and Building Emergency Management Capacity during the 2014–2016 Ebola Epidemic — Liberia, Sierra Leone, and Guinea." *MMWR Supplements* 65, no. 3 (July 8, 2016): 28–34. https://doi.org/10.15585/mmwr.su6503a5.

Closser, Svea. "Why Eradicating Polio Is More Complicated than It Seems." *SAPIENS*, July 11, 2018. https://www.sapiens.org/culture/polio-eradication-pakistan.

Douedari, Yazan, and Natasha Howard. "Perspectives on Rebuilding Health System Governance in Opposition-Controlled Syria: A Qualitative Study." *International Journal of Health Policy and Management* 8, no. 4 (January 9, 2019): 233–44. https://doi.org/10.15171/ijhpm.2018.132.

Forsgren, Lena, Fabrizio Tediosi, Karl Blanchet, and Dell D Saulnier. "Health Systems Resilience in Practice: A Scoping Review to Identify Strategies for Building Resilience." *BMC Health Services Research* 22, no. 1 (September 19, 2022). https://doi.org/10.1186/s12913-022-08544-8.

Ghafoor, Shazia, and Nadeem Sheikh. "Eradication and Current Status of Poliomyelitis in Pakistan: Ground Realities." *Journal of Immunology Research* 2016 (2016): 1–6. https://doi.org/10.1155/2016/6837824.

Hearn, Jeff, Sofia Strid, Anne Laure Humbert, and Dag Balkmar. "Violence Regimes: A Useful Concept for Social Politics, Social Analysis, and Social Theory." *Theory and Society* 51 (February 7, 2022). https://doi.org/10.1007/s11186-022-09474-4.

Hoffman, Frank. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies, 2007. ttps://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf.

Kanwal, Sumaira, Abrar Hussain, Shazia Mannan, and Shazia Perveen. "Regression in Polio Eradication in Pakistan: A National Tragedy." *Journal of the Pakistan Medical Association* 66, no. 3 (March 2016): 328–33. https://www.researchgate.net/publication/297715432_Regression_in_polio_eradication_in_Pakistan_A_national_tragedy.

Karo, Basel, Christopher Haskew, Ali S. Khan, Jonathan A. Polonsky, Md Khadimul Anam Mazhar, and Nilesh Buddha. "World Health Organization Early Warning, Alert and Response System in the Rohingya Crisis, Bangladesh, 2017–2018." *Emerging Infectious Diseases* 24, no. 11 (November 2018): 2074–76. https://doi.org/10.3201/eid2411.181237.

Kavulikirwa, Olivier Kambere. "Intersecting Realities: Exploring the Nexus between Armed Conflicts in Eastern Democratic Republic of the Congo and Global Health." *One Health* 19 (2024): 100849. https://doi.org/10.1016/j.onehlt.2024.100849.

Khan, Aurangzaib. "Polio: What's behind the Refusals?" *Dawn*, September 29, 2019. https://www.dawn.com/news/1507831.

Khan, Yasmin, Tracey O'Sullivan, Adalsteinn Brown, Shannon Tracey, Jennifer Gibson, Mélissa Généreux, Bonnie Henry, and Brian Schwartz. "Public Health Emergency Preparedness: A Framework to Promote Resilience." *BMC Public Health* 18, no. 1 (December 2019). https://doi.org/10.1186/s12889-018-6250-7.

Meier, Benjamin Mason, Hannah Rice, and Shashika Bandara. "Monitoring Attacks on Health Care as a Basis to Facilitate Accountability for Human Rights Violations." *Health and Human Rights* 23, no. 1 (June 2021): 55. https://pmc.ncbi.nlm.nih.gov/articles/PMC8233025.

Moturi, Edna K, Kimberly A Porter, Steven GF Wassilak, Rudolf H Tangermann, Ousmane M Diop, Cara C Burns, and Hamid Jafari. "Progress toward Polio Eradication — Worldwide, 2013–2014." *Morbidity and Mortality Weekly Report* 63, no. 21 (May 30, 2014): 468. https://pmc.ncbi.nlm.nih.gov/articles/PMC5779464.

Murali, Gopireddy, Mohan Reddy, Tayyaba Shaikh, E. Sreejit, Sonal Mehta, Naikmal Hamdard, Shabnam Sawganed, et al. "Action Plan Open Access Digitally Strengthened, Midwife-Led Intervention to Reach the Unreached Mothers across Ten Conflict-Prone Provinces of Afghanistan during Humanitarian Crisis." *Nursing and Midwifery Studies* 12, no. 2 (June 2023). https://doi.org/10.48307/NMS.2023.175273.

Njuguna, Charles, Mohamed Vandi, Tushar Singh, Ian Njeru, Jane Githuku, Wilson Gachari, Robert Musoke, et al. "Improving Global Health Security through

Implementation of the National Action Plan for Health Security in Sierra Leone, 2018–2021: Lessons from the Field." *BMC Public Health* 23, no. 2178 (2023). https://doi.org/10.1186/s12889-023-17103-7.

Nwafor, Chioma Dan, Elsie Ilori, Adebola Olayinka, Chinwe Ochu, Rosemary Olorundare, Edwin Edeh, Tochi Okwor, et al. "The One Health Approach to Incident Management of the 2019 Lassa Fever Outbreak Response in Nigeria." *One Health*13 (December 2021): 100346. https://doi.org/10.1016/j.onehlt.2021.100346.

Orris, Greta J., Pamela Dunlap, John Wallis, and Jeff Wynn. *Phosphate Occurrence and Potential in the Region of Afghanistan, Including Parts of China, Iran, Pakistan, Tajikistan, Turkmenistan, and Uzbekistan*. *Open-File Report*, 2015. https://doi.org/10.3133/ofr20151121.

Reem Ladadwa, Mahmoud Hariri, Muhammed Mansur Alatras, Yasir Elferruh, Abdulhakim Ramadan, Mahmoud Dowah, Yahya Mohammad Bawaneh, et al. "Health Information Management Systems and Practices in Conflict-Affected Settings: The Case of Northwest Syria." *Globalization and Health* 20, no. 1 (June 6, 2024). https://doi.org/10.1186/s12992-024-01052-w.

Shafiq, Yasir, Ameer Muhammad, Kantesh Kumar, Zabin Wajid Ali, Saba Noor, Zamir Hussain Suhag, Rehman Tahir, et al. "Toward Resilient Maternal, Neonatal and Child Health Care: A Qualitative Study Involving Afghan Refugee Women in Pakistan." *Health Services Insights* 18 (2025). https://doi.org/10.1177/11786329241310733.

Shakeel, Shahella Idrees, Matthew Brown, Shakeel Sethi, and Tim K. Mackey. "Achieving the End Game: Employing 'Vaccine Diplomacy' to Eradicate Polio in Pakistan." *BMC Public Health* 19, no. 1 (2019). https://doi.org/10.1186/s12889-019-6393-1.

Sparrow, Annie, Khaled Almilaji, Bachir Tajaldin, Nicholas Teodoro, and Paul Langton. "Cholera in the Time of War: Implications of Weak Surveillance in Syria for the WHO's Preparedness — a Comparison of Two Monitoring Systems." *BMJ Global Health* 1, no. 3 (October 2016): e000029. https://doi.org/10.1136/bmjgh-2016-000029.

SteelFisher, Gillian K, Robert J Blendon, Sherine Guirguis, Amanda Brulé, Narayani Lasala-Blanco, Michael Coleman, Vincent Petit, et al. "Threats to Polio Eradication in High-Conflict Areas in Pakistan and Nigeria: A Polling Study of Caregivers of Children Younger than 5 Years." *The Lancet Infectious Diseases* 15, no. 10 (October 2015): 1183–92. https://doi.org/10.1016/s1473-3099(15)00178-4.

Tekin, Fatih Cemal, and Fatma Selcen Ocal. "Attacks on Health Care Worldwide: 5-Year Review." *Eurasian Journal of Emergency Medicine* 22, no. 4 (December 1, 2023): 211–16. https://doi.org/10.4274/eajem.galenos.2023.42223.

Wahid, Braira, Babita Kumari, Khaled Mohammed Saifullah, and Muhammad Idrees. "The History and Current Killings of Polio Vaccinators in Pakistan: A Need for Targeted Surveillance Strategy." *Asia-Pacific Journal of Public Health* (2023): 10105395231158866. https://doi.org/10.1177/10105395231158866.

World Health Organization. *ERF Emergency Response Framework: Internal WHO Procedures*. Geneva: World Health Organization, 2024. https://iris.who.int/bitstream/handle/10665/375964/9789240058064-eng.pdf?sequence=1.

World Health Organization. *EWARS in a Box: Electronic Early Warning, Alert, and Response System in Emergencies*. Geneva: World Health Organization, n.d. https://cdn.who.int/media/docs/default-source/documents/emergencies/ewars-presentation.pdf.World Health Organization. *Health Emergency and Disaster Risk Management Framework*. Geneva: World Health Organization, 2019. https://iris.who.int/bitstream/handle/10665/326106/9789241516181-eng.pdf?sequence=1.

World Health Organization. "International Health Regulations." *WHO.int*. Last modified 2024. https://www.who.int/health-topics/international-health-regulations.

World Health Organization. "Surveillance in Emergencies." World Health Organization, 2023. https://www.who.int/emergencies/surveillance.

World Health Organization. *10 Proposals to Build a Safer World Together: Strengthening the Global Architecture for Health Emergency Preparedness, Response and Resilience*. Geneva: World Health Organization, 2022. https://cdn.who.int/media/docs/default-source/emergency-preparedness/who_hepr_june-30draftforconsult.pdf.

Youde, Jeremy. "The International Health Regulations." *Biopolitical Surveillance and Public Health in International Politics*, 2010, 147–75. https://doi.org/10.1057/9780230104785_7.

3

How Weaponized Migration has Informed the Kremlin's Disinformation Campaigns from 2015–2023

Kenneth McDANIEL

Abstract: This paper examines how weaponized migration has been exploited in Russia's disinformation campaigns to destabilize Western political cohesion. By analyzing the European Migration Crisis of 2015 and the Ukraine-Russia War in 2023, the study highlights how socio-political narratives surrounding migration have been manipulated to inflame divisions within NATO and the United States. The findings demonstrate that weaponized migration is not just a border crisis — it's an information weapon aimed at eroding trust, amplifying polarization, and weakening collective response to global threats.

Keywords: Weaponized Migration, Russia, Disinformation Campaigns, European Migration Crisis

Introduction

Helping to redefine international relations and domestic policies within an increasingly conventional strategy-transcending geopolitical landscape is weaponized migration — menacing, subtle, and powerful. The deliberate manipulation of human migration flows to achieve political, strategic, or

military objectives has evolved into a sophisticated tactic that reshapes both international dynamics and internal state stability. Among the practitioners of this approach, Russia stands out for its calculated and multi-layered use of migration within broader disinformation campaigns.

This tactic involves the exploitation of both real and perceived pressures on social services, employment opportunities, and national identity — intentionally fanning the flames of public anxiety and polarizing political discourse. Strategically timed leaks and media coverage often coincide with surges in migration, crafting narratives designed to maximize societal disruption. Migrants become more than pawns — they become unwitting agents in psychological operations engineered to fracture social cohesion and manipulate political outcomes.

These operations are particularly effective during periods of political instability or economic uncertainty, where national anxieties are already heightened. In such contexts, Russia not only disrupts internal affairs but also tests the resilience of targeted states, exploiting crises to project power without direct military intervention. By maintaining plausible deniability, the Kremlin avoids overt conflict while sowing chaos and deepening geopolitical divisions. The weaponization of migration during the 2015 European Migration Crisis and the ongoing Ukraine-Russian War represents a potent evolution in Russia's hybrid warfare playbook, where forced displacement is used both tactically and narratively.

This research investigates the convergence of Russia's disinformation operations and its manipulation of migratory flows as tools of hybrid warfare. It explores the following questions: In what ways did the weaponization of migration shape and inform the Kremlin's disinformation campaigns between 2015 and 2023? How did this exploitation influence the rise of right-wing extremism in Europe? And what can a comparative case study reveal about the trajectory of Russia's future information warfare strategies?

This paper argues that from 2015 to 2023, the Kremlin systematically weaponized migration to amplify disinformation, manipulate domestic politics in Europe, and fracture Western unity — transforming displaced

populations into instruments of psychological and geopolitical warfare. Grounded in securitization theory and Kelly Greenhill's concept of "Weapons of Mass Migration," the analysis situates Russia's tactics within the broader framework of strategic engineered migration.[79] Greenhill defines weaponized migration as the intentional use of population movements to coerce or destabilize other states by exploiting their political divisions, economic limitations, or social tensions.[80] This framework offers a valuable lens through which to understand Russia's hybrid strategies in both the 2015 migration crisis and the 2022 invasion of Ukraine.

Historical Background

Europe experienced a wave of new refugees and migrants requesting asylum in 2015. Most of the asylum seekers who arrived in Europe in 2015 were fleeing war and persecution from countries such as Syria, Afghanistan, and Iraq. Each was involved in their own related conflicts respectively; namely the Libyan Civil War, Syrian Civil War, and the 2014–2017 War in Iraq.

Thus, the European Crisis in 2015 counted an estimated 1,005,504 new arrivals into Europe.[81] Due to Russia's in-depth involvement in Syria, many analysts argued that Russian involvement in Syria, while brutal, was more focused on aiding Assad than deliberately exacerbating European migration pressures. At the time, the influx of migrants posed such an urgent challenge that allegations of weaponized migration received little scrutiny.

---

[79] See, for example, Kelly Greenhill, *Migration as a Weapon in Theory and in Practice* (Cambridge, MA: Belfer Center for Science and International Affairs, December 2016), https://www.belfercenter.org/publication/migration-weapon-theory-and-practice; Kelly Greenhill, "When Migrants Become Weapons," *Foreign Affairs* 101 (2022), https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals%2Fffora101&id=373; Nathan D. Steger, *The Weaponization of Migration: Examining Migration as a 21st Century Tool of Political Warfare* (December 1, 2014), Internet Archive, https://archive.org/details/theweaponization1094556815.

[80] Kelly Greenhill, *Migration as a Weapon in Theory and in Practice* (Cambridge, MA: Belfer Center for Science and International Affairs, December 2016), https://www.belfercenter.org/publication/migration-weapon-theory-and-practice.

[81] International Organization for Migration, "Irregular Migrant, Refugee Arrivals in Europe Top One Million in 2015: IOM," *International Organization for Migration*, December 22, 2015, https://www.iom.int/news/irregular-migrant-refugee-arrivals-europe-top-one-million-2015-iom.

However, in 2019, Schoemaker revisits the issue, acknowledging that while Russian actions may have influenced refugee flows, evidence of a deliberate strategy to weaponize migration remains circumstantial and unproven.[82] This has not stopped the U.S. General Breedlove from discerning that Russia intentionally fueled migration as part of hybrid warfare tactics to destabilize the EU. Even years later, whether Russia intentionally exacerbated migration remains a debated topic.[83] However, the extent to which Russian active measures capitalized on the crisis to weaponize the influx of migrants continues to warrant further investigation.

With Europe facing the migration crises, Russia used the instrument of refugee flows effectively in order to evoke pressures for creating fissures and instability in Europe. It is not a policy under ordinary migration but is closely linked with the strategies of disinformation in order to exploit fault lines within societies. During that time, the disinformation activity through the Russian governmental media and social media was also at its peak by portraying immigrants as criminals and holding them responsible for harming cultural integrity.[84] Such portrayals were designed to stir up xenophobic sentiment and feed ultra-right groups in European countries. These narratives were intelligently amplified during the most important electoral cycles, multiplying their potential impact on national politics and public opinion. Centered on immigration issues, Kremlin-backed propaganda effectively capitalized on societal fears and thus prejudices already existent within societies, finally opening the road to political groups sympathetic to Russia's interests or at least skeptic about the EU integration policies. By generating fear and social tension, Russia bolsters pro-Kremlin actors whose actions contribute to a broader interference campaign aimed at discrediting European governments and destabilizing the EU amid Russia's

---

[82] Schoemaker, Willem. *"Allegations of Russian Weaponized Migration Against the EU." Militaire Spectator* 188, no. 7/8 (2019). https://militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%207-8-2019%20Schoemaker.pdf.

[83] U.S. European Command. *"Gen. Breedlove's Hearing with the House Armed Services Committee."* Last modified 2016. Accessed July 30, 2025. https://www.eucom.mil/transcript/35355/gen-breedloves-hearing-with-the-house-armed-services-committee.

[84] Antonios Nestoras, *How the Kremlin Is Manipulating the Refugee Crisis* (Brussels: Wilfried Martens Centre for European Studies, January 2019), https://www.iedonline.eu/download/2019/IED-Research-Paper-Russia-as-a-security-provider_January2019.pdf.

conflict with Ukraine.[85] The targeted disinformation activities of this kind are therefore related to the growing right-wing extremism all over Europe.

In 2023, the Kremlin's activities intensified, but further deterioration of the relations between Ukraine and Russia again pushed migration as a strategic tool in this frozen conflict. This shift underlines how the actions are part of broader strategic goals and not some random acts. The conflict has caused millions of Ukrainians to flee across the European borders in search of safety. In response, Russian propaganda has exploited these refugee situations, constructing narratives that delegitimize Ukrainian leadership as well as exposing supposed inconsistencies in Western policies.[86] By using migration strategically, it helps burden European resources, while also acting as leverage within larger Russian disinformation operations to manipulate global geopolitical views. This paper investigates how the Kremlin exploits managed migration as a tool for gathering intelligence on internal socio-political climates, subsequently integrating that information into broader disinformation campaigns. Additionally, it explores how these tactics influence international relations through the complex interplay between forced human movement and orchestrated information warfare. Weaponized migration has long been a fixture in Russia's strategic arsenal — now amplified by the contextual backdrop of the 2015 European migration crisis and the ongoing war in Ukraine as of 2023.

European Migration Crisis 2015

By injecting controversial and emotionally charged narratives into the public discourse, Russian state media and social media platforms sowed discord and heightened tensions among European populations. According to "The Disconnective Power of Disinformation Campaigns," disinformation

---

[85] John Irish, "European Election: How the EU Says Russia Is Spreading Disinformation," *Reuters*, June 3, 2024, https://www.reuters.com/world/europe/european-election-how-eu-says-russia-is-spreading-disinformation-2024-06-03.

[86] Human Rights First. *"New Report Documents Russia's Disinformation Campaign against Ukraine."* Accessed July 19, 2024. https://humanrightsfirst.org/library/new-report-documents-russias-disinformation-campaign-against-ukraine.

campaigns "sustain a discursive conflict between users of social networks" and "sabotage horizontal connections between individuals on either side of a conflict".[87] Russia's disinformation campaigns during the migration crisis were meticulously crafted to exploit and exacerbate existing societal divisions within European countries. This approach aimed to fracture social cohesion and erode trust in democratic institutions.

A primary tactic was to depict migrants as a significant threat to European security and cultural identity. Russian media propagated stories portraying refugees as criminals and extremists, contributing to a climate of fear and hostility. These narratives were designed to appeal to emotions and leverage conflict-related social categorization, further dividing communities along ideological lines. The same paper highlights how such disinformation "contributes to the increasing impact of conflict-related social categorization on social ties".[88] This strategy not only inflamed public sentiment against migrants but also deepened societal rifts, making it easier for far-right ideologies to gain traction.

Support for Anti-Immigrant Parties

Russia's disinformation efforts have also played a crucial role in bolstering far-right, anti-immigrant parties across Europe. The Russians learned that by amplifying anti-immigrant rhetoric, Russian media enhanced the appeal of parties that shared a nationalist and Eurosceptic agenda. This became part of a broader strategy to weaken the European Union's political cohesion and undermine its capacity to present a unified front against Russian aggression. The article "Strange Bedfellows: Putin and Europe's Far Right" notes that "closer ties with rising political parties in the EU will give Putin more leverage against NATO."[89] Supporting pre-existing grassroots

---

[87] Gregory Asmolov, "The Disconnective Power of Disinformation Campaigns," *Journal of International Affairs* 71, no. 1.5 (September 2018): 69–76.

[88] Asmolov, "Disconnective Power of Disinformation," 72.

[89] Alina Polyakova, *Strange Bedfellows: Putin and Europe's Far Right*, Institute of Modern Russia, 2014, https://gale.com/ps/i.do?id=GALE%7CA384341263.

movements has thus become a means to influence European politics in favor of Russian interests.

Moreover, the strategic alliance between Russia and far-right European parties was underpinned by shared anti-American and anti-EU sentiments. The same source explains that "behind Russia's affection for Le Pen and her fellow travelers may lie something more than appreciation for her endorsement of Crimea: a shared anti-Americanism."[90] By promoting these established parties, Russia aimed to erode the political stability of the EU and create a more favorable geopolitical landscape for itself.

Framing Migration Issues to Benefit Russia's Geopolitical Goals

The Russian disinformation campaign utilized three main narratives around the refugee crisis: guilt, threat, and security. These narratives were carefully constructed to serve Russia's broader geopolitical objectives. The article "How the Kremlin is manipulating the Refugee Crisis Russian Disinformation as a Threat to European Security" outlines these narratives: a "guilt narrative" accusing the West of causing the refugee crisis, a "threat narrative" emphasizing the security risks posed by refugees, and a "security narrative" positioning Russia as a potential security provider for Europe.[91]

By framing the refugee crisis as a consequence of Western policies, Russia aimed to discredit the EU and the US. The "threat narrative" focused on the alleged dangers of mass migration, aiming to stir public fear and bolster support for policies that aligned with Russian interests. Finally, the "security narrative" presented Russia as a stabilizing force, capable of addressing the crisis more effectively than the West. This multifaceted approach not only undermined the credibility of Western governments but also sought to position Russia as an alternative power broker in European security affairs. These narratives are not incidental but are part of what German

[90] Ibid.

[91] Nestoras, *How the Kremlin Is Manipulating the Refugee Crisis*.

officials call "Putin's toolbox of disinformation," a suite of coordinated strategies that includes the manipulation of migration themes to provoke public outrage, polarize societies, and erode democratic resilience.[92]

Russia's disinformation efforts were particularly effective in Eastern European countries, where anti-immigrant sentiments and skepticism towards the EU were already prevalent. Peter Pomerantsev argues, the Kremlin's information war operates by flooding the information space with conflicting messages, conspiracy theories, and emotionally charged content, leaving audiences confused and distrustful of all sources.[93] The same article notes that "a nexus of alt-right online media outlets relayed this message in Hungary, Slovakia, and the Czech Republic among other countries, where the right-wing parties have many times resonated with disinformation material originating in Russia".[94] By targeting these regions, Russia aimed to exploit existing political and social vulnerabilities to its advantage.

Ukraine-Russian War

Looking deeper into Russia's efforts, intensifying with the full-scale invasion of Ukraine in 2022 and continuing past 2023; the Ukraine-Russia War has not only caused the displacement of millions of refugees into Europe but has also provided fertile ground for Russia to further sophisticate their disinformation campaigns. This massive migration has placed additional strain on European Union (EU) countries, exacerbating internal tensions and resource allocation issues not dissimilar to. According to the European Council on Foreign Relations (ECFR), as of November 2023,

---

[92] "'Putins Werkzeugkasten der Desinformation': Bundesregierung," *Die Bundesregierung*, March 9, 2022, https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/desinformation-interview-ead-2010706.

[93] Peter Pomerantsev, "Authoritarianism Goes Global (II): The Kremlin's Information War," *Journal of Democracy* 26, no. 4 (October 2015): 40–50, https://www.journalofdemocracy.org/articles/authoritarianism-goes-global-ii-the-kremlins-information-war.

[94] Nestoras, Antonios. How the Kremlin is manipulating the refugee crisis…, January 2019. https://www.iedonline.eu/download/2019/IED-Research-Paper-Russia-as-a-security-provider_January201 9.pdf.

over 4 million people who fled Ukraine remained in the EU, with Germany and Poland hosting the largest numbers.[95] Wojnowski argues that this coercive migration engineers a blend of psychological warfare and hybrid destabilization, aimed specifically at overburdening border states such as Poland and Lithuania while testing NATO's institutional and humanitarian resilience.[96] This displacement has been a key vector for Russia's disinformation campaigns, as the influx of refugees stokes pre-existing anxieties about migration in host countries.

Russian media has adeptly used the plight of Ukrainian refugees to shape narratives that serve its geopolitical goals. By portraying the Ukrainian government as ineffective and the West as hypocritical in its response to the crisis, Russian disinformation aims to weaken support for Ukraine, amplify internal divisions within the EU, and legitimize their actions.[97] This type of propaganda is not just pervasive — it is also effective. A 2021 study on pro-Kremlin disinformation in Ukraine found that even brief exposure to false narratives significantly decreased trust in media and democratic institutions, illustrating the psychological reach of such campaigns.[98] However, Russia propaganda isn't the only one to target Ukraine and migrants fleeing from the region. Alberto-Horst Neidhardt and Paul Butcher conducted a research from 2019–2020 indicating Russia-linked sources such as RT and Sputnik accounted for only a small proportion of online disinformation, while the same hostile narratives appeared on

---

[95] Mireia Faro Sarrats, "Fear and Fatigue: Why Anti-Migrant Sentiment in Europe Helps Russia," *European Council on Foreign Relations (ECFR)*, January 22, 2024, https://ecfr.eu/article/fear-and-fatigue-why-anti-migrant-sentiment-in-europe-helps-russia.

[96] Michał Wojnowski, "The Genesis, Theory, and Practice of Russian Coercive Migration Engineering: A Contribution to the Study of the Migration Crisis on NATO's Eastern Flank," *Przegląd Bezpieczeństwa Wewnętrznego* 14, no. 26 (May 11, 2022): 263–300, https://doi.org/10.4467/20801335pbw.21.042.15702.

[97] "Desinformation als Waffe im russischen Angriffskrieg auf die Ukraine," *Die Bundesregierung informiert*, February 10, 2023, https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/desinformation-als-waffe-2167604; "Russische Desinformationskampagnen," *Die Bundesregierung informiert*, August 30, 2022, https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/aus-narrativen-desinformation-2080112.

[98] Aaron Erlich and Calvin Garner, "Is Pro-Kremlin Disinformation Effective? Evidence from Ukraine," *The International Journal of Press/Politics* 26, no. 4 (2021): 797–814, https://doi.org/10.1177/19401612211045221.

large numbers from domestic European websites and blogs.[99] This has not stopped the ECFR from highlighting how Russian propaganda builds on European anxieties about migration to stoke resistance to Ukrainian refugees, exploiting the "cost of living crisis" to create a narrative that these refugees are unwelcome and a burden.[100] Russian disinformation campaigns actively ignite local tensions to the point where the domestic media writes the disinformation itself.

Far-Right Alliances and Anti-Immigrant Sentiment

Russia's ties with far-right political parties in Europe, which often share anti-immigrant views, have been instrumental in its disinformation strategy. These alliances enable Russia to amplify anti-immigrant sentiment and create social divisions within European countries. For example, in Poland, recent criminal reports involving Ukrainian refugees have proved to be false: Russia is fueling xenophobia and resistance to immigration.[101] Russia's strategic use of disinformation during the annexation of Crimea in 2014 set a precedent for its current tactics. By denying military involvement and sowing confusion during critical military stages, Russia blurred the lines between enemy and non-enemy, war and peace.[102] This same strategy was even tested previously during the European Migration Crisis a year later and proved to be more effective, where disinformation about Ukrainian refugees creates uncertainty and divides public opinion.

---

[99] Alberto-Horst Neidhardt and Paul Butcher, "Disinformation on Migration: How Lies, Half-Truths, and Mischaracterizations Spread," *Migration Policy Institute*, September 8, 2022, https://www.migrationpolicy.org/article/how-disinformation-fake-news-migration-spreads.

[100] Mireia Faro Sarrats, "Fear and Fatigue: Why Anti-Migrant Sentiment in Europe Helps Russia," *European Council on Foreign Relations (ECFR)*, January 22, 2024, https://ecfr.eu/article/fear-and-fatigue-why-anti-migrant-sentiment-in-europe-helps-russia.

[101] Ibid.; "Desinformation als hybride Bedrohung: Bundesregierung," *Die Bundesregierung*, August 31, 2023, https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/cybersicherheit-desinformation-1872752.

[102] Yevgeniy Golovchenko, "Measuring the Scope of Pro-Kremlin Disinformation on Twitter," *Nature Communications*, December 11, 2020, https://www.nature.com/articles/s41599-020-00659-9.

For instance, the Kremlin's disinformation campaigns portray the EU and the US as incapable of managing the refugee crisis, thereby positioning Russia as a more reliable security provider.

Russian disinformation campaigns aim to create and exploit social divisions within Europe by framing migration issues in ways that benefit Russia's geopolitical goals. The disinformation narratives include a "guilt narrative" accusing the West of causing the refugee crisis, a "threat narrative" about the lack of security due to migration, and a "security narrative" that presents Russia as an alternative security provider.[103] These narratives are disseminated through state-owned media and a nexus of alt-right online media outlets, particularly targeting Eastern European countries where right-wing parties resonate with such material.

Undermining EU Unity and Migration Policies

By fostering anti-immigrant sentiment and supporting far-right political parties, Russian disinformation campaigns aim to undermine EU unity on migration policies. This phenomenon has prompted formal EU concern: a 2021 Think Tank analysis highlights the convergence between foreign and domestic disinformation efforts targeting migrants.[104] This strategy not only weakens the EU's collective response to the refugee crisis but also aligns with Russia's broader revisionist agenda to disrupt the post-Cold War order in Europe. The rise of Eurosceptic and anti-American parties in Europe, bolstered by Russian disinformation, paves the way for Russia's return as a significant security provider in Central and Eastern Europe.[105]

---

[103] Antonios Nestoras, *How the Kremlin Is Manipulating the Refugee Crisis*, IED Research Paper, January 2019, https://www.iedonline.eu/download/2019/IED-Research-Paper-Russia-as-a-security-provider_January2019.pdf.

[104] Judit Szakács and Éva Bognár, *The Impact of Disinformation Campaigns about Migrants and Minority Groups in the EU*, Think Tank: European Parliament, 2021, https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2021)653641.

[105] Nestoras, *How the Kremlin Is Manipulating the Refugee Crisis*.

Continuities and Differences

Nathan Steger characterizes the weaponization of migration as a 21st-century form of political warfare, in which states and actors deliberately manipulate refugee flows to destabilize adversaries or achieve coercive outcomes.[106] This framing situates Russia's use of migration during the 2015 crisis and the Ukraine war as part of a broader tradition of asymmetric tools in hybrid conflict. Putting both cases together, in both crises, Russian disinformation campaigns aimed to amplify social division by stoking fears about refugees and migrants, however, the world has witnessed a new focus on Russia's immediate geopolitical objectives using disinformation campaigns as a means to undermine support for Ukraine independence and weaken NATO's response on Russia's militaristic actions. With Russia having consistently supported far-right and Eurosceptic political parties, it is not strange that it has become a staple in today's strategy to isolate Ukraine from the rest of the world. Russia has been able to exploit both crises to destabilize Europe, amplify social divisions, and further its own geopolitical goals. The Kremlin's Disinformation campaigns has organized and benefited from the influx of refugees into other countries thus Russia has weaponized migrants and refugees alike.

Conclusion

The Kremlin's disinformation campaign in the Ukraine-Russian War is the culmination of years of experience which could only be refined from the weaponized migration they have used. Russia's weaponization of migration through disinformation campaigns has been a deliberate and strategic effort to achieve its geopolitical objectives. By refining its tactics over time, Russia has successfully manipulated public opinion, supported far-right movements, and undermined the political cohesion of its adversaries. The lessons learned from the European Migration Crisis were applied and

---

[106] Nathan D. Steger, *The Weaponization of Migration: Examining Migration as a 21st Century Tool of Political Warfare* (December 1, 2014), Internet Archive, https://archive.org/details/theweaponization1094556815.

expanded upon during the Ukraine-Russia War, demonstrating Russia's ability to adapt and enhance its disinformation campaigns. The Kremlin's disinformation campaign is a testament to the power of information warfare in shaping international relations and influencing domestic politics. As Russia continues to exploit migration and other societal vulnerabilities, it remains crucial for Europe and the broader international community to develop robust countermeasures to protect democratic institutions and maintain geopolitical stability.

The broader implications of Russia's actions underscore the need for a comprehensive and coordinated response from the international community. Enhancing media literacy, strengthening cybersecurity measures, and fostering cross-border cooperation are essential steps in countering the threat posed by disinformation. Additionally, addressing the root causes of migration and supporting vulnerable populations can help mitigate the impact of weaponized migration. As the world navigates an increasingly complex information landscape, understanding and countering the strategies employed by actors like Russia is vital for safeguarding democratic values and ensuring global security.

Bibliography

"Allegations of Russian Weaponized Migration Against the EU." *Militaire Spectator*, 2019. https://militairespectator.nl/sites/default/files/uitgaven/inhoudsopgave/Militaire%20Spectator%207-8-2019%20Schoemaker.pdf.

Asmolov, Gregory. "The Disconnective Power of Disinformation Campaigns." *Journal of International Affairs* 71, no. 1.5 (September 2018): 69–76.

Butcher, Paul, and Alberto-Horst Neidhardt. "Disinformation on Migration: How Lies, Half-Truths, and Mischaracterizations Spread." *Migration Policy Institute*, September 8, 2022. https://www.migrationpolicy.org/article/how-disinformation-fake-news-migration-spreads.

"Desinformation als Hybride Bedrohung: Bundesregierung." *Die Bundesregierung informiert*, August 31, 2023. https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/cybersicherheit-desinformation-1872752.

"Desinformation als Waffe im Russischen Angriffskrieg auf die Ukraine." *Die Bundesregierung informiert*, February 10, 2023. https://www.bundesregierung.de/bregde/schwerpunkte/umgang-mit-desinformation/desinformation-als-waffe-2167604.

Erlich, Aaron, and Calvin Garner. "Is Pro-Kremlin Disinformation Effective? Evidence from Ukraine." *Journalism & Mass Communication Quarterly*, 2021. https://journals.sagepub.com/doi/full/10.1177/19401612211045221.

Golovchenko, Yevgeniy. "Measuring the Scope of Pro-Kremlin Disinformation on Twitter." *Nature Humanities and Social Sciences Communications*, December 11, 2020. https://www.nature.com/articles/s41599-020-00659-9.

Greenhill, Kelly. "Migration as a Weapon in Theory and in Practice." *Belfer Center for Science and International Affairs*, December 2016. https://www.belfercenter.org/publication/migration-weapon-theory-and-practice.

"When Migrants Become Weapons." *Foreign Affairs*, 2022. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals%2Ffora101&id=373.

"Gen. Breedlove's Hearing with the House Armed Services Committee." *EUCOM*, 2016. https://www.eucom.mil/transcript/35355/gen-breedloves-hearing-with-the-house-armed-services-committee.

International Organization for Migration. "Irregular Migrant, Refugee Arrivals in Europe Top One Million in 2015: IOM." December 22, 2015. https://www.iom.int/news/irregular-migrant-refugee-arrivals-europe-top-one-million-2015-iom.

Irish, John. "European Election: How the EU Says Russia Is Spreading Disinformation." *Reuters*, June 3, 2024. https://www.reuters.com/world/europe/european-election-how-eu-says-russia-is-spreading-disinformation-2024-06-03.

Nestoras, Antonios. "How the Kremlin Is Manipulating the Refugee Crisis." *Institute of European Democrats*, January 2019. https://www.iedonline.eu/download/2019/IED-Research-Paper-Russia-as-a-security-provider_January2019.pdf.

"New Report Documents Russia's Disinformation Campaign Against Ukraine." *Human Rights First*. Accessed July 19, 2024. https://humanrightsfirst.org/library/new-report-documents-russias-disinformation-campaign-against-ukraine.

Polyakova, Alina. "Strange Bedfellows: Putin and Europe's Far Right." *World Affairs*, 2014. https://go.gale.com/ps/i.do?id=GALE%7CA384341263.

Pomerantsev, Peter. "Authoritarianism Goes Global (II): The Kremlin's Information War." *Journal of Democracy*, 2015. https://www.journalofdemocracy.org/articles/authoritarianism-goes-global-ii-the-kremlins-information-war.

"Putins Werkzeugkasten der Desinformation." *Die Bundesregierung informiert*, March 9, 2022. https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/desinformation-interview-ead-2010706.

"Russische Desinformationskampagnen." *Die Bundesregierung informiert*, August 30, 2022. https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/aus-narrativen-desinformation-2080112.

Sarrats, Mireia Faro. "Fear and Fatigue: Why Anti-Migrant Sentiment in Europe Helps Russia."*European Council on Foreign Relations (ECFR)*, January 22, 2024. https://ecfr.eu/article/fear-and-fatigue-why-anti-migrant-sentiment-in-europe-helps-russia.

Steger, Nathan. "The Weaponization of Migration: Examining Migration as a 21st Century Tool of Political Warfare." *Internet Archive*, December 1, 2014. https://archive.org/details/theweaponization1094556815.

Szakács, Judit, and Éva Bognár. "The Impact of Disinformation Campaigns About Migrants and Minority Groups in the EU." *European Parliament Think Tank*, 2021. https://www.europarl.europa.eu/thinktank/en/document/EXPO_IDA(2021)653641.

Wojnowski, Michał. "The Genesis, Theory, and Practice of Russian Coercive Migration Engineering." *Przegląd Bezpieczeństwa Wewnętrznego* 14, no. 26 (May 11, 2022): 263–300. https://doi.org/10.4467/20801335pbw.21.042.15702.

4

Between Symbol and Strategy: Gendered Violence in Terrorism

Cayla CHUN

Abstract: Terrorist organizations intentionally weaponize gender to assert ideological dominance, destabilize societies, and fracture communities. Boko Haram's 2014 abduction of schoolgirls in Chibok, Nigeria, exemplifies how violence against women operates as a deliberate tactic that is rooted in systemic gender inequality, state neglect, and the symbolic power of women's bodies. Through qualitative analysis, the research examines how terroristic gender-based violence acts to reinforce control and weaken communal resilience. Additionally, the research amplifies women-led resistance movements that reclaim agency and reconceptualize security discourse. Women-led, survivor-centered counterterrorism strategies emerge as urgent and essential to sustainable policy reform.

Keywords: Gender-based violence, Boko Haram, terrorism, women in conflict, symbolic violence

Introduction: The Weaponization of Gender in Terrorism

The deliberate targeting of women and girls by terrorist organizations is a frightening manifestation of the intersection between patriarchal violence and political extremism. The interplay between extremist violence and entrenched gender hierarchies reveals the calculated logic behind

how terrorist groups exploit women's societal vulnerabilities for ideological, tactical, and symbolic purposes. Utilizing the case of Boko Haram's 2014 kidnapping of schoolgirls in Chibok, Nigeria, this paper investigates why women and girls are disproportionately targeted by terrorist organizations and what structural factors heighten their susceptibility.

Although there is substantial research on terrorism, gender-based violence, and women in conflict, these fields are often explored in isolation. Terrorism studies have traditionally emphasized operational tactics, ideological motivations, or state-centric analyses, often sidelining the role of gender.[107] Meanwhile, earlier gender-based violence literature tended to portray violence against women as a byproduct of war or a breakdown of social order.[108] The United Nations defines gendered-based violence as, "harmful acts directed at an individual based on their gender" including sexual violence, forced marriage, trafficking, and other abuses rooted in structural inequalities and power imbalances.[109] Increasingly, scholars argue that such violence, like rape, is not incidental but can serve as serve as a deliberate tactic used by armed groups to promote cohesion, instill fear, and assert dominance.[110] Yet even as gendered-based violence is progressively recognized as a tactic of war, terrorism studies have been slow to fully integrate this framework. When women appear in terrorism literature, they are often cast in narratives as either passive victims or active perpetrators, without adequate attention to why women and girls are systemically targeted.[111] This paper addresses that gap by bridging gendered-based violence theory with terrorism studies to examine how terrorist organizations,

---

[107] Richard Jackson. *The Case for Critical Terrorism Studies* (2007), http://hdl.handle.net/2160/1945.

[108] Amani El Jack, Emma Bell, and Lata Narayanaswamy. *Gender & Armed Conflict* (Brighton: BRIDGE, 2003).

[109] UNHCR US. "Gender-Based Violence," accessed July 25, 2025, https://www.unhcr.org/us/what-we-do/protect-human-rights/protection/gender-based-violence.

[110] Dara Kay Cohen. "Explaining Rape during Civil War: Cross-National Evidence (1980–2009)," *American Political Science Review* 107, no. 3 (2013): 461–77, https://doi.org/10.1017/s0003055413000221.

[111] Caron E. Gentry, and Laura Sjoberg. *Beyond Mothers, Monsters, Whores: Thinking about Women's Violence in Global Politics* (London: Bloomsbury Academic & Professional, 2015), http://ebookcentral.proquest.com/lib/stolaf-ebooks/detail.action?docID=2146956.

specifically Boko Haram, intentionally weaponize gender not just to inflict harm, but to assert ideological dominance, destabilize communities, and exploit systemic inequality.

This paper contends that the strategic targeting of women and girls by terrorist organizations stems from a nexus of systemic gender inequality, state neglect, and the symbolic value of women's bodies within ideological warfare. Through a close examination of academic literature and the Chibok case study, this paper aims to uncover how gender is weaponized in asymmetrical conflict, what this reveals about broader social structure, and what long-term consequences such violence imposes. Finally, the paper concludes by emphasizing women-led resistance and urging for policy initiatives that center women's agency and inclusion in counterterrorism strategies.

Methodology

This paper utilizes a qualitative approach by drawing from scholarly literature as well as primary accounts and reports surrounding Boko Haram's intentional gendered violence through the kidnapping of Chibok schoolgirls in Northern Nigeria. In 2014, members of Boko Haram raided a secondary school where over two hundred girls were completing final exams. Specifically, 276 sixteen to eighteen-year-old girls were kidnapped and trafficked through the Sambisa Forest, where they faced numerous human rights abuses.[112] Today, it is estimated that over one hundred of these girls remain missing.[113] This case was chosen as a main point of analysis for the intentional weaponization of gender in terrorism because it is a clear example of how terrorist organizations deliberately use gendered violence to advance ideological goals, gain global attention, and weaken communities; it especially allows for the examination of systemic

[112] Human Rights Watch. *"Those Terrible Weeks in Their Camp": Boko Haram Violence against Women and Girls in Northeast Nigeria* (New York, 2014).

[113] *"The ABC of Our Demands."* #BringBackOurGirls, accessed June 30, 2025, https://bringbackourgirls.ng/our-demands.

gender inequality, lack of government protection, and the symbolic role of women in society create conditions of vulnerability.

Structural Vulnerabilities: Gender Inequalities and State Neglect

One of the primary enablers of terroristic gender-based violence in conflict-affected regions is systemic gender inequality. Globally, women are often viewed through a stereotypical lens as the weaker sex, and this assumption motivates terrorist organizations to wreak havoc on societies by weaponizing gender.[114] For example, Boko Haram's treatment of women draws directly from the degraded status of women in Nigerian society in combination with the existing patriarchal infrastructure.[115] Examples of such deep-seated gender inequalities in Nigeria include "female genital mutilation, the practice of purdah that prevails within the Muslim community whereby women are secluded from public observation, and the discrimination of widows".[116] Furthermore, in many parts of Northern Nigeria, girls' education is already under threat due to the sociocultural norms that prioritize boys' education and enforce early marriage.[117] The existence of these societal gender inequalities creates culturally ingrained norms that undermine the empowerment of girls and women by causing them to suffer from economic manipulation, sexual exploitation, and political marginalization.[118] However, this context not only renders women and girls vulnerable to general insecurity but also to targeted attacks by groups like Boko Haram, who exploit these gender hierarchies. Boko Haram's and

---

[114] Taiwo O. Adefisoye and Niyi O. Adedokun, *"Driven to the Mainstream: Women and Girls in International Terrorism," European Journal of Social Sciences Studies*, no. 0 (April 28, 2019), https://doi.org/10.46827/ejsss.v0i0.539.

[115] Temitope Oriola, *"'Unwilling Cocoons': Boko Haram's War Against Women," Studies in Conflict and Terrorism* 40, no. 2 (2017): 99–121, https://doi.org/10.1080/1057610X.2016.1177998.

[116] Mok Shen Yang, *"Conflict and Violence against Women and Girls: Gender-Based Violence and the Boko Haram in Nigeria," Global and Policy Journal of International Relations* 3, no. 2 (January 12, 2015): 46, https://doi.org/10.33005/jgp.v3i02.1934.

[117] Ibid.

[118] Ibid.

other terrorist organizations' intentional choice to target women in acts of terror, like the kidnapping of the Chibok schoolgirls, is an extension of the "repertoire of violence" and systemic gender inequality that is entrenched throughout the sociopolitical and cultural areas of operation.[119]

Far from incidental, government negligence to uphold basic societal protections has created an enabling environment for targeted terroristic gendered-based violence to persist. Defined as the failure of government institutions to provide adequate security or protection to all populations, state neglect creates conditions of vulnerability that terrorist organizations, like Boko Haram, exploit.[120] In Nigeria and the broader Sahel region, high poverty, weak infrastructure, underfunded education systems, and ineffective policing reflect chronic institutional failure. For instance, the average Sahelian individual lives on less than $1.25 USD per day, which illustrates widespread socioeconomic deprivation.[121] These systemic deficiencies not only deepen general insecurity but disproportionately endanger women and girls, who are often left without adequate protection, justice, or services. Furthermore, despite Nigeria's ratification of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) in 1985, the treaty remains largely unenforced in Nigerian courts.[122] The failure to uphold international commitments further exacerbates state neglect, especially in areas of education, gender based violence, and survivor protection. Particularly, Boko Haram's ideological opposition to Western-style education for girls thrives within this environment, and the Nigerian government's lack of protection regarding girls' right to education, exemplified by their failure to secure the Chibok secondary school in 2014, demonstrates how state neglect magnifies the gendered impacts of violence. Additionally,

---

[119] Oriola, *"'Unwilling Cocoons,'"* 100.

[120] Nina Käsehage, "Female Vulnerabilities for Terrorist Activities in the Sahel Zone," in *Terrorism and Political Contention*, ed. J. Besenyő, L. Issaev, and A. Korotayev (Cham: Springer, 2024), 63–75, https://doi.org/10.1007/978-3-031-53429-4_4.

[121] Ibid.

[122] *"CEDAW/C/NGA/CO/7-8: Concluding Observations on the Combined Seventh and Eighth Periodic Reports of Nigeria."* OHCHR, accessed July 3, 2025, https://www.ohchr.org/en/documents/concluding-observations/cedawcngaco7-8-concluding-observations-combined-seventh-and.

during times of intra-state conflict, the increase in the absence of male family members and the heightened presence of hostile armed actors in civilian areas magnifies the vulnerability of women and girls.[123] Overall, state neglect is not merely a backdrop to violence, but rather an active, structural enabler of strategic gender-based targeting of women by terrorist organizations.

Ideological and Symbolic Violence: Women's Bodies as Battlegrounds

Symbolic violence plays a significant part in the strategic targeting of women by terrorist groups, thereby turning their bodies into instruments of ideological warfare. The 2014 abduction of the Chibok schoolgirls by Boko Haram was not only a tactical operation but a deeply symbolic act. Boko Haram explicitly opposes Western-style education, particularly for girls, because they view it as a corrupting force against Islamic values and traditional gender hierarchies. In a public statement, Boko Haram's leader Abubakar Shekau explicitly declared that "Western education is entirely sinful" and warned that girls should return to their homes, stating that "in Islam, it is permissible to abduct infidel women".[124] As a result, the attack on the Chibok school became a powerful gesture that violently rejected modernity and gender equality.

Women are seen as bearers of cultural symbols like honor, bloodlines, and communal identity, which makes them especially vulnerable to violence intended to destabilize or humiliate entire populations. By controlling, violating, or appropriating female bodies, terrorist groups assert dominance over community identities.[125] Furthermore, many societies associate women's bodies with familial and societal dignity, particularly in relation to

---

[123] Mok, *"Conflict and Violence against Women and Girls,"* 46.

[124] Abdelwahab El-Affendi and Salisu Gumel, *"Abducting Modernity: Boko Haram, Gender Violence and the Marketplace of Bigotry," Hawwa* 13, no. 2 (2015): 135, https://doi.org/10.1163/15692086-12341274.

[125] Dara, "Explaining Rape during Civil War: Cross-National Evidence (1980–2009)".

sexual purity.[126] In such contexts, rape, abduction, and forced marriage are not merely physical violations but symbolic attacks. Strategic violence and rape in conflict zones position women as "metaphors for a defeated community," and violations of their bodies serve to demoralize the broader group by transmitting messages of terror and intimidation to men and the wider population.[127] In gender-based violence terrorism, the defilement of women is a means of terrorizing the rest of the population as a way to crush their resistance.

Particularly, in Boko Haram's case, abducting and forcibly marrying the Chibok schoolgirls served to destabilize familial and cultural structures while broadcasting the group's ideological defiance to women's education. Their intentional targeting of schoolgirls underscores the group's belief that women embody the cultural and religious identity of their communities, and therefore, attacking them is equivalent to attacking the community itself.[128] Through this lens, women become proxies in a broader ideological battle, and gender-based violence becomes a deliberate strategy to assert control, spread fear, and claim moral and cultural superiority. This transformation of violence into a spectacle reinforces the group's ideological message while inflicting profound psychological and political trauma on communities and individuals already made vulnerable by state neglect and systemic inequality.

Long Term Consequences: Trauma, Stigma, and Societal Disruption

The physical and psychological trauma inflicted on abducted women and girls is profound. After being abducted, many women and girls face many human rights abuses like forced labor, arranged marriage, and sexual

[126] Taiwo O. Adefisoye and Niyi O. Adedokun, *"Driven to the Mainstream: Women and Girls in International Terrorism," European Journal of Social Sciences Studies*, no. 0 (April 28, 2019). https://doi.org/10.46827/ejsss.v0i0.539.

[127] Mok, *"Conflict and Violence against Women and Girls,"* 44.

[128] Ibid.

violence.[129] As a result, survivors often suffer from post-traumatic stress disorder, sexual violence-related injuries, and prolonged captivity effects.[130] A nineteen-year-old survivor of the Chibok kidnappings describes, "It is just the memories. I can't shut them out. Even in sleep, it is like I'm back there and everything is still happening".[131] While this testimony powerfully reflects individual trauma, it also reveals how the psychological residue of violence continues to control survivors after their captivity has ended. These long-term effects are compounded by the fact that none of the kidnapping survivors reported receiving information about how to access post-sexual violence medical care, such as treatment for injury, emergency contraception, or post-exposure prophylaxis to prevent HIV.[132]

Beyond individual suffering, there are collective ramifications, including many girls who returned home were ostracized by local society and deemed "tainted" due to their association with Boko Haram. As a result, girls returning home after abduction are often rejected by their families and communities. One nineteen year old woman, raped during abduction, said she could not bring herself to tell her husband what had happened; another survivor feared disclosure would destroy her chance at marriage.[133] Oftentimes, community members and Nigerian soldiers refer to surviving women and girls as "Boko Haram wives"; women reported feeling ostracized as their communities refused to interact, look, or touch them as people feared diseases.[134] Furthermore, social workers in Borno and Adamawa states described how families, fearing communal shame, went as far as to relocate survivors to distant towns to avoid judgment or

---

[129] "Nigeria: Girls Failed by Authorities after Escaping Boko Haram Captivity – New Report," *Amnesty International* (blog), June 9, 2024, https://www.amnesty.org/en/latest/news/2024/06/nigeria-girls-failed-by-authorities-after-escaping-boko-haram-captivity-new-report.

[130] "'Help Us Build Our Lives': Girl Survivors of Boko Haram and Military Abuses in North-East Nigeria," *Amnesty International* (blog), June 9, 2024, https://www.amnesty.org/en/documents/afr44/7883/2024/en.

[131] Human Rights Watch, ed., *"Those Terrible Weeks in Their Camp": Boko Haram Violence against Women and Girls in Northeast Nigeria*, 43.

[132] Ibid.

[133] Human Rights Watch, *"Those Terrible Weeks in Their Camp."*

[134] "'*Help Us Build Our Lives*.'"

expulsion by neighbors.[135] This secondary victimization, where survivors face discrimination instead of support, perpetuates cycles of gender inequality. The culture of silence around rape, coupled with the absence of accessible psychosocial care, prevents healing and reinforces patriarchal norms that treat women as repositories of communal honor rather than autonomous individuals.

However, the consequences of terrorism's gendered-based violence extend well beyond the individual. Survivors' exclusion from education and employment undermines not only their own futures but the social and economic recovery of their communities. Trauma and shame fracture families, while the normalization of violence against women destabilizes social trust. Moreover, these dynamics deepen mistrust between citizens and the state, whose failure to prevent such atrocities or to adequately care for victims afterward intensifies the sense of abandonment.[136] Such consequences make it imperative to view these attacks not as isolated incidents but as part of a broader system of structural and symbolic control.

Resistance and Reconceptualizing Security: Women as Agents of Change

Despite the profound trauma and systemic failures surrounding gendered-based violence in terrorism, women have emerged as powerful agents of resistance, resilience, and transformation. The *Bring Back Our Girls* movement, led by Nigerian women activists in response to the 2014 Chibok abductions, demands action and accountability in the safe return of all kidnapped Chibok schoolgirls and the prevention of future terroristic gendered-based violence atrocities in Nigeria.[137] The grassroots movement fostered international attention; it served as a key factor in

---

[135] Human Rights Watch, *"Those Terrible Weeks in Their Camp."*

[136] *"'Help Us Build Our Lives.'"*

[137] *"The ABC of Our Demands."* #BringBackOurGirls. Accessed July 3, 2025, https://bringbackourgirls.ng/our-demands.

forcing the Nigerian government and the larger global community to confront the scale and gendered nature of Boko Haram's and other terrorist organizations' violence.[138] *Bring Back Our Girls* allowed for powerful local mobilization that simultaneously demanded the return of the abducted girls while challenging the narrative of women as mere victims, and therefore asserting their place as leaders in security discourse and political action.

This form of women-led resistance underscores the urgency of transforming how security is conceptualized and implemented. Instead of viewing security solely through militarized or top-down state responses, it must be reimagined as a people-centered process that addresses the lived realities of those most affected. Specifically in the case of terroristic gendered-based violence, as recognized in United Nations Resolution 1325, women hold intimate knowledge of the harms inflicted and the solutions needed.[139] Their exclusion from policy-making not only undermines the legitimacy of counterterrorism efforts but also misses critical opportunities for more community-driven, sustainable solutions. The intentional engagement of women and girls in conflict resolution and counterterrorism efforts gives them not only a voice but also a sense of shared responsibility and agency in rebuilding social trust.[140] Inclusion must go beyond surface-level representation; it must involve active participation in shaping trauma-informed reintegration programs, educational opportunities, and long-term strategies that confront structural inequalities.

Finally, recognizing the gendered dimensions of violence is critical for addressing immediate harm and preventing future cycles of instability. Reconceptualizing security in post-conflict societies must go beyond physical reconstruction to include the restoration of autonomy and voice

---

[138] Adekalu Samuel Olutokunbo et al., *"Bring Back Our Girls, Social Mobilization: Implications for Cross-Cultural Research,"* 2015.

[139] United Nations Security Council. *Resolution 1325 (2000) on Women and Peace and Security.* S/RES/1325 (2000). New York: United Nations, 2000, https://documents.un.org/doc/undoc/gen/n00/720/18/pdf/n0072018.pdf.

[140] Taiwo O. Adefisoye and Niyi O. Adedokun, *"Driven to the Mainstream: Women and Girls in International Terrorism," European Journal of Social Sciences Studies*, no. 0 (April 28, 2019), https://doi.org/10.46827/ejsss.v0i0.539.

for women and girls. Their leadership and lived experiences are indispensable for creating increasingly just, inclusive, and sustainable counterterrorism practices.

Conclusion

This paper has argued that the disproportionate targeting of women and girls by terrorist organizations is intentional. The deliberate terroristic choice is rooted in systemic gender inequality, enabled by state neglect, and amplified through symbolic violence that attacks both bodies and identities. Using the Chibok schoolgirl abductions as a case study, this analysis has illustrated how terrorist violence exploits gendered vulnerabilities to achieve ideological and tactical goals. Recognizing this strategic use of gendered-based violence by terrorist organizations is essential for developing effective counterterrorism practices and advancing global human rights. If counterterrorism efforts fail to account for the gendered dimensions of violence, they risk perpetuating the very inequalities that fuel extremist narratives. However, some limitations of this paper remain. This research focuses on one case and one region, which may limit generalizability. Further research could explore other contexts, such as ISIS's use of women as both perpetrators and victims, or the gendered dynamic of terrorism in Southeast Asia or Latin America. Policy implications include the urgent need to integrate gender into counterterrorism strategies, prioritize survivor-centered support programs, and fund initiatives that empower women and girls in conflict zones. Long-term solutions require a shift from viewing women solely as victims to recognizing their leadership in shaping resilient, inclusive, and secure societies. Ultimately, combating terrorism must also mean dismantling the structural vulnerabilities that make gendered-based violence a viable strategy; only by doing so can we address both the symptoms and the root causes of such deeply embedded harm.

Bibliography

Adefisoye, Taiwo O., and Niyi O. Adedokun. 2019. "DRIVEN TO THE MAINSTREAM: WOMEN AND GIRLS IN INTERNATIONAL TERRORISM." *European Journal of Social Sciences Studies*, no. 0 (April). https://doi.org/10.46827/ejsss.v0i0.539.

"CEDAW/C/NGA/CO/7-8: Concluding Observations on the Combined Seventh and Eighth Periodic Reports of Nigeria." n.d. OHCHR. Accessed July 3, 2025. https://www.ohchr.org/en/documents/concluding-observations/cedawcngaco7-8-concluding-observations-combined-seventh-and.

Cohen, Dara Kay. "Explaining Rape during Civil War: Cross-National Evidence (19802009)." *American Political Science Review* 107, no. 3 (2013): 461–77. https://doi.org/10.1017/s0003055413000221.

El-Affendi, Abdelwahab, and Salisu Gumel. 2015. "Abducting ModernityBoko Haram, Gender Violence and the Marketplace of Bigotry." *Hawwa* 13 (2): 127–40. https://doi.org/10.1163/15692086-12341274.

El Jack, Amani, Emma Bell, and Lata Narayanaswamy. 2003. *Gender & Armed Conflict*. Brighton: BRIDGE.

Gentry, Caron E., and Laura Sjoberg. 2015. *Beyond Mothers, Monsters, Whores: Thinking about Women's Violence in Global Politics*. Bloomsbury Academic & Professional. http://ebookcentral.proquest.com/lib/stolaf-books/detail.action?docID=2146956.

"Help Us Build Our Lives: Girl Survivors of Boko Haram and Military Abuses in North-East Nigeria." 2024. *Amnesty International* (blog). June 9, 2024. https://www.amnesty.org/en/documents/afr44/7883/2024/en.

Human Rights Watch, ed. 2014. *"Those Terrible Weeks in Their Camp": Boko Haram Violence against Women and Girls in Northeast Nigeria*. New York/N.Y.

Jackson, Dr Richard. 2007. *The Case for Critical Terrorism Studies*. http://hdl.handle.net/2160/1945.

Jackson, Richard. 2007. *The Case for Critical Terrorism Studies*. http://hdl.handle.net/2160/1945.

Käsehage, Nina. 2024. "Female Vulnerabilities for Terrorist Activities in the Sahel Zone." In *Terrorism and Political Contention*, 63–75. Springer, Cham. https://doi.org/10.1007/978-3-031-53429-4_4.

"Nigeria: Girls Failed by Authorities after Escaping Boko Haram Captivity — New Report." 2024. *Amnesty International* (blog). June 9, 2024. https://www.amnesty.org/en/latest/news/2024/06/nigeria-girls-failed-by-authorities-after-escaping-boko-haram-captivity-new-report.

Olutokunbo, Adekalu Samuel, Turiman Suandi, Oluwaseyitan Rotimi Cephas, and Irza Hanie Abu-Samah. 2015. “Bring Back Our Girls, Social Mobilization: Implications for Cross-Cultural Research.”

Oriola, Temitope. 2017. “‘Unwilling Cocoons’: Boko Haram’s War Against Women.” *Studies in Conflict and Terrorism, 40 (2),* 99–121. https://doi.org/10.1080/1057610X.2016.1177998.

“The ABC of Our Demands.” n.d. #Bring Back Our Girls Now. Accessed June 30, 2025. https://bringbackourgirls.ng/our-demands.

UNHCR US. n.d. “Gender-Based Violence.” Accessed July 25, 2025. https://www.unhcr.org/us/what-we-do/protect-human-rights/protection/gender-based-violence.

United Nations Security Council. 2000. Resolution 1325 (2000) on Women and Peace and Security. [S/RES/1325 (2000)] New York: United Nations. https://documents.un.org/doc/undoc/gen/n00/720/18/pdf/n0072018.pdf.

Yang, Mok Shen. 2015. “Conflict and Violence against Women and Girls: Gender-Based Violence and the Boko Haram in Nigeria.” *Global and Policy Journal of International Relations* 3 (02). https://doi.org/10.33005/jgp.v3i02.1934.

5

How Political Attitudes Toward Ukrainian Refugees and State Unpreparedness Shape Refugees' Vulnerability to Exploitation

Audra SONI

Abstract: The Russian invasion of Ukraine has displaced millions of people, triggering a humanitarian crisis that has increased the risk of gender based violence (GBV) and human trafficking. This paper examines the impact of shifts in the sentiment of Polish citizenry, Polish political rhetoric, and migration policies on the safety of Ukrainian refugees. Drawing on data from NGOs, UNHCR reports, news coverage, and migration-focused organizations, the research finds that while Poland initially demonstrated strong support for Ukrainian refugees, growing humanitarian fatigue, shifts in public opinion, and increased xenophobia towards refugees have contributed to an increase in vulnerability to human trafficking and GBV. These conditions have disproportionately increased the risk of exploitation among women and children. This paper also highlights the erosion of temporary protection frameworks and a widening disconnect between civil society efforts and governmental support. Understanding these dynamics is crucial for designing sustainable, resilient, and inclusive refugee protection strategies and counter-trafficking policies in prolonged displacement contexts.

Keywords: Gender Based Violence (GBV), Human trafficking, Top-down policies, Refugee, Humanitarian Fatigue, Vulnerability

Introduction

Armed conflict often leads to mass displacement, placing vulnerable populations at risk of exploitation, including gender based violence (GBV), sexual exploitation, and labor trafficking. Russia's invasion of Ukraine on February 24, 2022, has resulted in approximately four million internally displaced people and over seven million refugees across Europe.[141] While labor trafficking mostly targets men, women and girls disproportionately face sexual exploitation.[142] The political and social environments in which refugees find themselves play a critical role in either mitigating or exacerbating risks to their safety in their host country. In the early stages of the Russian invasion, Poland responded with generous aid programs, offering housing, education, healthcare, and temporary protection to Ukrainian refugees.[143] However, amid broader shifts in EU migration policy and growing humanitarian fatigue, public and political sympathy in Poland waned, and support structures grew tired.[144] The research in this paper is particularly important when considering global stability. Although core Polish policies toward Ukrainian refugees have largely remained in place, shifting political rhetoric and decreasing public sympathy have weakened support systems and enforcement of protection mechanisms, contributing to greater exploitation, trafficking, and GBV.

---

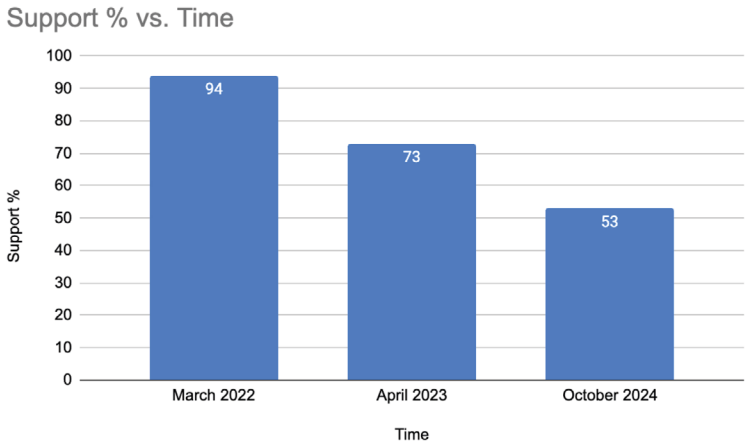
[141] *"Ukraine Crisis Response."* International Organization for Migration. Accessed June 24, 2025. https://www.iom.int/crisis-ukraine#:~:text=An%20estimated%203.7%20million%20people,in%20desperate%20need%20of%20support. Accessed 24 June 2025.

[142] Daphne Panayotatos, Irla Atanda, and Eric Schwartz, "*Crisis in Ukraine: Humanitarian and Human Rights Imperatives*," Refugees International, March 21, 2022, https://www.refugeesinternational.org/reports-briefs/crisis-in-ukraine-humanitarian-and-human-rights-imperatives.

[143] "*Temporary Protection Poland*," European Council on Refugees and Exiles (AIDA), n.d., https://asylumineurope.org/wp-content/uploads/2013/06/AIDA-PL_Temporary-Protection_2022.pdf.

[144] "*Ukrainians in Poland and the War in Ukraine*." CBOS (Public Opinion Research Center), October 2024, https://www.cbos.pl/PL/publikacje/public_opinion/2024/10_2024.pdf.

Figure 2: Polish Citizen Support for Aid for Ukrainian Refugees



Source: https://www.cbos.pl/PL/publikacje/public_opinion/2024/10_2024.pdf.

Background — Russian Invasion of Ukraine

The initial Russian invasion of Ukraine began in February 2014, when Russia invaded and then annexed Crimea. Afterward, from 2015 to 2018, there was increased labor migration from Ukraine to Poland because of better salaries and work opportunities across the border.[145] On February 24, 2022, Russia launched another invasion of Ukraine, which resulted in an enormous refugee flow into the rest of Europe.

Over four million Ukrainian refugees fled the conflict within a couple of months.[146] The majority of those refugees were women and children because men aged 18–60 were not allowed to leave Ukraine during wartime due to martial law.[147] These women and children are naturally more vulnerable to exploitation and GBV, a demographic reality that is essential

[145] Viktoriia Kutsaya, *interview by Audra Soni*, June 17, 2025.

[146] Rachel Amran, "*US Embassy: Ukraine May No Longer Allow Men with Dual Citizenship Leave Country*," *The Kyiv Independent*, June 5, 2024, https://kyivindependent.com/us-embassy-in-ukraine-men-with-dual-citizenship-will-no-longer-be-able-to-leave-the-country.

[147] Ibid.

to consider when assessing their safety and protection needs in a host country. In total, almost seven million Ukrainian refugees have fled the conflict. Germany, Poland, and the Czech Republic host the highest number of Ukrainian refugees in the European Union.[148]

When Ukrainian refugees first arrived in Poland, most were welcomed with essential supplies such as hygiene products, food, clothing, money, and baby care items. Polish citizens and NGOs mobilized rapidly, with many opening their homes and providing essential supplies and general welfare.[149] The humanitarian response was rapid and large in scale, but it ultimately exceeded institutional capacity. This led to fragmentation and a lack of coordination in aid distribution. The lack of centralized oversight made it difficult to ensure consistent standards of care and protection across different regions and organizations.[150]

Motivation Behind Russia's Invasion

Russia's President, Vladimir Putin, has masterfully manipulated the messaging on the invasion, varying the story depending on the audience. The Kremlin has spread disinformation to justify the invasion of Ukraine. However, consistent themes, irrespective of audience, have been the Kremlin's concern over North Atlantic Treaty Organization (NATO) expansion, the need to protect Russian-speaking populations, and the goal to "demilitarize" and "de-Nazify" Ukraine.[151] The disinformation about Ukraine as a "Nazi state" is strategic since as many as 24 million Russians

---

[148] *"Vulnerability to Trafficking in Persons in the Context of the War in Ukraine: Findings from Poland and Romania."* International Organization for Migration, n.d., https://eca.iom.int/sites/g/files/tmzbdl2626/files/documents/2024-09/vulnerability-to-tip_war-in-ukraine_poland-and-romania_august-2024.pdf.

[149] Vanessa Gera, "*Poland Once Threw Its Doors Open to Millions of Ukrainian Refugees, but the Mood Has Shifted*," *AP News*, May 11, 2025, https://apnews.com/article/poland-ukrainians-presidential-election-4982cc03f7b5a88c8e21cc340087e7e8.

[150] Rebecca Panayotatos, Tolu Atanda, and Melissa Schwartz, *"Crisis in Ukraine: Humanitarian and Human Rights Imperatives."* Refugees International, [date]. https://[insert URL].

[151] Paul Kirby, "*Why Did Putin's Russia Invade Ukraine*?," *BBC*, March 18, 2025, https://www.bbc.com/news/articles/cj0q964851po.

died directly or indirectly from the Nazi invasion in WWII.[152] This memory remains a stinging reminder among Russian citizens. Putin's claim that Russian speakers in Ukraine require protection from the Kyiv government is a clear propaganda tactic intended to delegitimize Ukraine's democratically elected, pro-Western president, Volodymyr Zelenskyy, and provide a legitimate, however untrue, basis for Russia's invasion. This "self-defense" argument helps limit global military support for the Ukrainian government, making it easier for the Kremlin to fight Ukraine. According to the BBC, the Kremlin wants to "destroy Ukraine politically by destroying the head of state."[153] These narratives spread disinformation campaigns with the intention of trying to manipulate audiences to Putin's side.

These falsehoods also aim to exploit both domestic and international perceptions, providing a distraction from the extreme humanitarian toll of the conflict and deflecting attention from the war's true political motives.[154] Russia's invasion strategy has not been limited to bombing military sites and targeting soldiers. It has involved deliberate, cruel, and unlawful attacks on civilian infrastructure, including homes, hospitals, schools, and power plants.[155] These actions are not accidental but form part of a broader strategy designed to inflict widespread hardship, destabilization, and fear among the civilian population. Rather than relying solely on traditional military tactics, Putin is deliberately employing hybrid warfare, which combines physical attacks with cyber operations, disinformation, and other tools aimed at undermining both Ukrainian society and international support.[156]

---

[152] "*Research Starters: Worldwide Deaths in World War II*," The National WWII Museum | New Orleans, 2024, https://www.nationalww2museum.org/students-teachers/student-resources/research-starters/research-starters-worldwide-deaths-world-war.

[153] Kirby, "*Why Did Putin's Russia Invade Ukraine*?".

[154] Ibid.

[155] Peter Dickinson, "*Russian Hybrid Warfare: Ukraine's Success Offers Lessons for Europe*," Atlantic Council, June 5, 2025, https://www.atlanticcouncil.org/blogs/ukrainealert/russian-hybrid-warfare-europe-should-study-ukraines-unique-experience.

[156] Ibid.

Polish Policy Evolution and Humanitarian Fatigue

In March 2022, the European Union activated the Temporary Protection Directive (TPD) for the first time since its creation in 2001, granting Ukrainian refugees immediate legal status and access to fundamental, essential services across member states. In line with this, Poland passed the Law on Assistance to Citizens of Ukraine in Connection with Armed Conflict on the Territory of that Country, offering visa-free entry, the right to work, and access to healthcare, education, and social benefits. The act also provided temporary protection for up to 18 months, with the possibility of extension, making Poland one of the most generous host countries at the outset of the crisis.[157] However, despite honorable intentions, because both Polish citizens and the Polish government had largely refused to host refugees during the 2015 Syrian crisis, Poland lacked the institutional infrastructure and experience necessary to manage a large-scale influx.[158] Unlike some Western European countries, Poland was less equipped with sustainable, organized systems for refugee reception. As a consequence, the arrival of millions of Ukrainian refugees in 2022 resulted in an improvised, uncoordinated, and heavily volunteer-led response.[159]

Poland's early generosity in supporting Ukrainian refugees was, however, not sustainable. As the crisis persisted, the political discourse around migration began to shift. Migration became increasingly politicized, with politicians framing it as a resource burden rather than a humanitarian obligation. President-elect Karol Nawrocki and many of his supporters emphasized slogans such as "Poland First" and argued that public funds should prioritize domestic welfare over refugee aid. This rhetoric was shown in statements such as, "Let's help others, but let's take care of our own citizens first."[160]

---

[157] "*Temporary Protection Poland*," European Council on Refugees and Exiles.

[158] Brianna Navarre, "*Inside Poland's Drastic Immigration Reversal*," *US News & World Report*, March 8, 2022), https://www.usnews.com/news/best-countries/articles/2022-03-08/the-russia-ukraine-conflict-highlights-polands-complicated-history-with-refugees.

[159] Ibid.

[160] Anna Wlodarczak-Semczuk and Justyna Pawlak, "*Who Is Poland's next President Karol Nawrocki?*," *Reuters*, June 2, 2025, https://www.reuters.com/world/europe/who-is-polands-next-president-karol-nawrocki-2025-06-02.

Public opinion also reflected this change: according to a Warsaw-based research center, support for assisting Ukrainian refugees declined from 94% in early 2022 to just 57% by December 2024, almost 40% in less than three years.[161] President-elect Karol Nawrocki has played a key role in reshaping the narrative, emphasizing national interest over international solidarity toward Ukrainian refugees. In a January 2025 statement, Nawrocki declared, "Ukraine does not treat us as a partner. It behaves in an indecent and ungrateful way in many respects," signaling a turn toward more nationalist rhetoric such as "Poland first" and "Protect our own first." He has also argued that Poland's commitment to refugee aid, while commendable, is unsustainable in the long term given domestic economic pressures.[162]

The politicization of migration is not unique to Poland. This sentiment reflects a broader trend across the EU. As refugee support places increasing strain on national budgets, economic anxieties have made public sentiment more subject to manipulation. Russian propaganda has sought to exploit these tensions, portraying Ukrainian refugees as ungrateful economic burdens to sow division within the EU and weaken support for Ukraine.[163] Humanitarian fatigue is particularly prominent in the most vulnerable host countries and among the most marginalized refugee populations, where limited resources and social strain compound existing risks of exploitation and exclusion.[164] Still, Poland remains one of the most generous countries in responding to the Ukrainian refugee crisis. Almost one million Ukrainian refugees currently reside in Poland, and about 17 million crossed into Poland before continuing to other destinations.[165]

---

[161] "*Ukrainians in Poland and the War in Ukraine*." CBOS (Public Opinion Research Center).

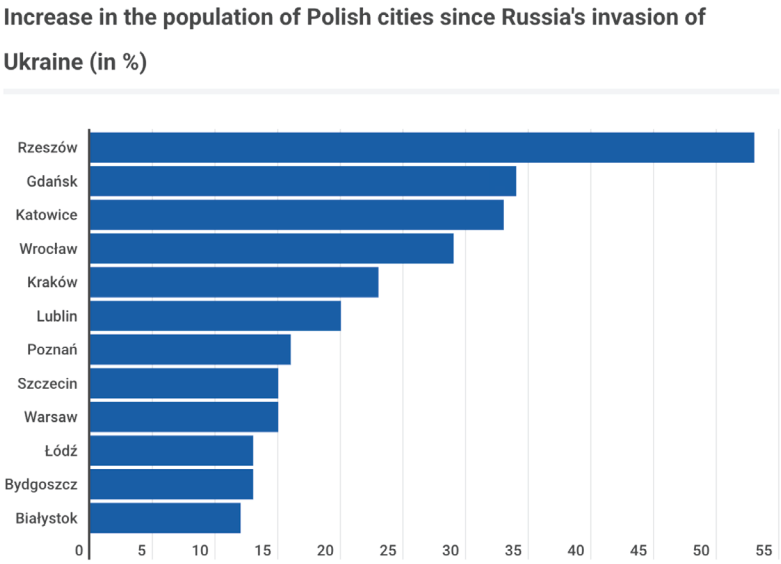
[162] Gera, "*Poland Once Threw Its Doors Open*."

[163] Raf Casert, *"EU Warns of 'Solidarity Fatigue' despite Warm Welcome for Millions of Ukraine Refugees," AP News*, June 6, 2023, https://apnews.com/article/eu-ukraine-refugees-solidarity-fatigue-russia-propaganda-0bfd0c6aa7538e8bd823923d82765c57.

[164] Casert, "*EU Warns of 'Solidarity Fatigue*.'"

[165] *"Poland."* Project HOPE, https://www.projecthope.org/region/europe/poland. Accessed 27 June 2025.

Figure 3: Increase in the Population of Polish Cities from Ukrainian Refugees



Source: https://www.eib.org/en/stories/ukrainian-poland-infrastructure-refugees.

Trafficking and GBV in Poland

These shifting political and public dynamics are not occurring in a vacuum. They directly impacted the practical safety of refugees on the ground, particularly in terms of exposure to trafficking and GBV. Russia's invasion of Ukraine led to the biggest refugee crisis since WWII.[166] War-driven displacement creates "ideal" conditions for traffickers, and vulnerability is worsened by financial instability, legal uncertainty, and social isolation.[167] These factors disproportionately affect women and children, who are the majority of Ukrainian refugees.[168] Refugees report being approached by

[166] "*OSCE and UN Special Reps Statement on Trafficking for the Purpose of Sexual Exploitation and Sexual Violence in the Context of War against Ukraine — Ukraine*," *ReliefWeb*, March 30, 2023, https://reliefweb.int/report/ukraine/osce-and-un-special-reps-statement-trafficking-purpose-sexual-exploitation-and-sexual-violence-context-war-against-ukraine.

[167] "*Vulnerability to Trafficking in Persons in the Context of the War in Ukraine*."

[168] Panayotatos, Atanda, and Schwartz, "*Crisis in Ukraine*."

men without official identification who offered questionable employment or housing.[169] While some individuals were able to recognize these offers as potentially exploitative, others, particularly those in distress or unfamiliar with local systems, were more vulnerable. Both refugee testimonies and reports from Human Rights Watch highlight the absence of systematic protection measures and security protocols in Poland during the early stages of the refugee influx, which substantially increased exposure to exploitation.[170]

Exploitation also occurs online, so digital prevention efforts must also be strengthened. This includes expanding public reporting mechanisms, improving platform accountability, and enforcing legal consequences for online exploitation. Since Russia's 2022 invasion of Ukraine, reports indicate a growing demand for exploitative online content featuring Ukrainian women.[171] This surge in demand incentivizes traffickers to target and recruit vulnerable female Ukrainian refugees for sexual exploitation, particularly through digital platforms where oversight remains limited or usually non-existent.[172]

In general, exploitation was exacerbated by the emergency scale and extraordinary speed of the Ukrainian refugee influx, which quickly overwhelmed existing Polish government systems. This made it difficult to coordinate and implement effective protective procedures. Although Poland had built some crisis response mechanisms to foster resilience, the magnitude and speed of the Ukrainian displacement exceeded those capacities.[173] As a result, the initial reception of refugees was primarily managed by well-meaning volunteers and civil society activists rather than trained professionals equipped to identify trafficking risks and educate refugees.[174] While these volunteers acted with compassion and urgency,

---

[169] Human Rights Watch, "Poland: Trafficking, Exploitation Risks for Refugees," *Human Rights Watch*, April 29, 2022, https://www.hrw.org/news/2022/04/29/poland-trafficking-exploitation-risks-refugees.

[170] Human Rights Watch, "Poland: Trafficking, Exploitation Risks for Refugees."

[171] "*OSCE and UN Special Reps Statement on Trafficking*."

[172] Ibid.

[173] Human Rights Watch, "*Poland: Trafficking, Exploitation Risks for Refugees*."

[174] Ibid.

they often lacked the specialized training required to recognize signs of vulnerability.[175] To ensure more comprehensive protection for displaced individuals and families, systematic training programs for volunteers are necessary. Properly trained volunteers could also serve as key intermediaries, disseminating information to refugees who would then share it within their communities.[176] While Poland implemented basic measures, such as public information campaigns, trafficking hotlines, and volunteer training programs, these efforts were often limited in scope and effectiveness.[177] More comprehensive and sustained approaches would have significantly enhanced the capacity to prevent and respond to exploitation. Additionally, providing holistic care that addresses the physical, psychological, emotional, and socioeconomic needs of survivors is essential. These integrated support systems are fundamental for recovery and for reducing the long-term vulnerability and increasing the mental health of displaced populations.[178]

Ultimately, the Polish government and its partner agencies lacked the capacity to thoroughly vet households offering shelter or individuals volunteering to provide private transportation.[179] This resulted in significant gaps in security and protection. In some cases, refugees said that the presence of police provided little more than symbolic reassurance, rather than active protection. Some stated that it looked like Polish police were "only there for show."[180]

Although the Polish government formally welcomed refugees from Ukraine, much of the responsibility for delivering basic, necessary services such as food, shelter, and transportation fell to nongovernmental organizations and individual citizens. These well-intentioned actors unfortunately operated without coordinated oversight or streamlined

---

175 Ibid.

176 Human Rights Watch, "*Poland: Trafficking, Exploitation Risks for Refugees*."

177 "OSCE and UN Special Reps Statement on Trafficking."

178 Ibid.

179 Human Rights Watch, "Poland: Trafficking, Exploitation Risks for Refugees."

180 Ibid.

endeavors.[181] The complexity of this type of response requires trained professionals and effective coordination. Poland was just not ready to handle this humanitarian crisis in a sustainable and optimal way.

The Role of Policy in Shaping Risk

Top-down policies from the Polish government have had tangible effects, both good and bad, on both Polish citizens and Ukrainian refugees. As the crisis has extended beyond its initial emergency phase, the needs of refugees have evolved from immediate access to food and shelter to long-term necessities such as steady employment, education, and healthcare.[182] In May 2022, the European Investment Bank (EIB) approved a €2 billion loan as part of a solidarity package for Ukraine.[183] A portion of this funding supported the creation of Poland's €600 million Aid Fund, administered by Bank Gospodarstwa Krajowego (BGK).[184] This fund was designed to finance programs that promote refugee integration and improve access to essential services, particularly for women and children — the majority demographic of those displaced. The establishment of the Aid Fund marked a significant step in institutionalizing and funding refugee support, especially as volunteer-driven efforts began to wane under the weight of humanitarian fatigue and resource depletion.[185]

As of 2025, Poland's current Prime Minister Donald Tusk has adopted a more restrictive stance toward migration, framing it primarily as a national security issue. In public statements, Tusk has warned that migration is being "weaponized" by hostile actors, particularly Belarus, and emphasized the need to ensure that Polish citizens feel secure within the country's

---

[181] Ibid.

[182] Dawid A Fusiek, "*A Solidarity Package Helps Poland Integrate Ukrainian Refugees*," *European Investment Bank,* November 28, 2022, https://www.eib.org/en/stories/ukrainian-poland-infrastructure-refugees.

[183] Ibid.

[184] Ibid.

[185] Fusiek, "*A Solidarity Package Helps Poland Integrate Ukrainian Refugees*."

borders.[186] "Migration," Tusk stated, "will not be a threat to the security of borders and citizens."[187] This rhetoric has translated into policy: in 2024, Poland issued 31% fewer migration visas across all categories compared to 2023, signaling a measurable shift in migration policy and public sympathy.[188] Rather than distinguishing between refugees fleeing war and other forms of migration, Tusk's policies position migration broadly as a political and security threat, an approach that risks dehumanizing displaced people and undermining collective responsibility in times of crisis.

Tusk has also been vocal about his desire to exert tighter control over who is allowed into Poland, stating that the government must know "who comes here, why, where, and how useful they are."[189] This utilitarian approach to migration prioritizes economic contribution and national interest over humanitarian obligations. Concurrently, Poland has ramped up its defense spending, allocating 4.3% of GDP to defense in 2024 and projecting 4.7% in 2025, one of the highest rates among NATO member states.[190] Some of this funding has been directed toward border security, further reinforcing the securitization of migration in Polish political discourse.[191]

Conclusion

The initial wave of support for Ukrainian refugees in Poland was characterized by remarkable compassion and solidarity. Citizens opened their homes, donated supplies, and mobilized en masse to help those fleeing war. However, over time, that deeply personal generosity gave way to exhaustion. As humanitarian and financial fatigue set in without

---

[186] "*Taking Back Control, Ensuring Security — the Chancellery of the Prime Minister — Gov.pl Website*," The Chancellery of the Prime Minister, 2024, https://www.gov.pl/web/primeminister/taking-back-control-ensuring-security.

[187] Ibid.

[188] Ibid.

[189] "*Taking Back Control, Ensuring Security*."

[190] Ibid.

[191] Ibid.

a hand-off to institutional welfare systems, and as political leaders increasingly framed migration as a threat rather than a humanitarian obligation, refugees were left more vulnerable. This shift in sentiment was especially dangerous for women and children, who make up the majority of Ukrainian refugees due to martial law, and are disproportionately at risk of trafficking and GBV.[192] The Russian invasion has displaced nearly seven million Ukrainians, testing the limits of humanitarian systems across Europe, especially in Poland, which has absorbed one of the largest amounts of refugees.[193] Despite initially leading in response efforts, Poland has not been immune to the pressures of economic strain, political polarization, and rising nationalistic political rhetoric. I saw this firsthand while living in Warsaw: in the faces of refugees navigating uncertain futures, in the protests that reflected a growing nationalism defined by racial and cultural exclusion, and in the growing rhetoric that casts displaced people as burdens rather than neighbors in need.

To prevent these patterns from repeating, future humanitarian responses must be durable and structural. Countries need coordinated, well-funded, and depoliticized aid systems that can withstand long-term displacement. Volunteers and frontline workers must be trained not just to offer immediate support, but to recognize and intervene in situations of potential exploitation over time. Beyond policy, nation-states must foster a societal culture that sees refugees not as temporary problems that will go away, but as human beings deserving of long-term safety, dignity, and community in their host countries. It is crucial that societies shift their lens from viewing refugee migration as a political and societal burden to seeing it as a very human issue that deserves support and empathy, because someday the shoe may be on the other foot. Poland is not alone in this challenge. Around the world, refugee crises are testing the resilience of societies. How we respond, whether with resilience and humanity or fatigue and fear will shape not only the futures of those displaced but the kind of societies we become.

---

[192] Panayotatos, Atanda, and Schwartz, "*Crisis in Ukraine*."

[193] "*Vulnerability to Trafficking in Persons in the Context of the War in Ukraine*."

Bibliography

Amran, Rachel. "US Embassy: Ukraine May No Longer Allow Men with Dual Citizenship to Leave Country." *The Kyiv Independent*, June 5, 2024. https://kyivindependent.com/us-embassy-in-ukraine-men-with-dual-citizenship-will-no-longer-be-able-to-leave-the-country.

Casert, Raf. "EU Warns of 'Solidarity Fatigue' despite Warm Welcome for Millions of Ukraine Refugees." *AP News*, June 6, 2023. https://apnews.com/article/eu-ukraine-refugees-solidarity-fatigue-russia-propaganda-0bfd0c6aa7538e8bd823923d82765c57.

Dickinson, Peter. "Russian Hybrid Warfare: Ukraine's Success Offers Lessons for Europe." *Atlantic Council*, June 5, 2025. https://www.atlanticcouncil.org/blogs/ukrainealert/russian-hybrid-warfare-europe-should-study-ukraines-unique-experience.

Fusiek, Dawid A. "A Solidarity Package Helps Poland Integrate Ukrainian Refugees." *European Investment Bank*, November 28, 2022. https://www.eib.org/en/stories/ukrainian-poland-infrastructure-refugees.

Gera, Vanessa. "Poland Once Threw Its Doors Open to Millions of Ukrainian Refugees, but the Mood Has Shifted." *AP News*, May 11, 2025. https://apnews.com/article/poland-ukrainians-presidential-election-4982cc03f7b5a88c8e21cc340087e7e8.

Human Rights Watch. "Poland: Trafficking, Exploitation Risks for Refugees." *Human Rights Watch*, April 29, 2022. https://www.hrw.org/news/2022/04/29/poland-trafficking-exploitation-risks-refugees.

International Organization for Migration (IOM). "Crisis in Ukraine." International Organization for Migration, 2023. https://www.iom.int/crisis-ukraine.

Kirby, Paul. "Why Did Putin's Russia Invade Ukraine?" *BBC*, March 18, 2025. https://www.bbc.com/news/articles/cj0q964851po.

Kutsaya, Viktoriia. Personal interview. June 17, 2025.

Navarre, Brianna. "Inside Poland's Drastic Immigration Reversal." *US News & World Report*, 2022. https://www.usnews.com/news/best-countries/articles/2022-03-08/the-russia-ukraine-conflict-highlights-polands-complicated-history-with-refugees.

OSCE and UN Special Representatives. "Statement on Trafficking for the Purpose of Sexual Exploitation and Sexual Violence in the Context of War against Ukraine." *ReliefWeb*, March 30, 2023. https://reliefweb.int/report/ukraine/osce-and-un-special-reps-statement-trafficking-purpose-sexual-exploitation-and-sexual-violence-context-war-against-ukraine.

Panayotatos, Daphne, Irla Atanda, and Eric Schwartz. "Crisis in Ukraine: Humanitarian and Human Rights Imperatives." *Refugees International*, March 21, 2022. https://www.refugeesinternational.org/reports-briefs/crisis-in-ukraine-humanitarian-and-human-rights-imperatives.

Project HOPE. "Poland." *Project HOPE*, May 12, 2024. https://www.projecthope.org/region/europe/poland.

The Chancellery of the Prime Minister. "Taking Back Control, Ensuring Security." *Gov.pl*, 2024. https://www.gov.pl/web/primeminister/taking-back-control-ensuring-security.

The National WWII Museum. "Research Starters: Worldwide Deaths in World War II." *The National WWII Museum* | New Orleans, 2024. https://www.nationalww2museum.org/students-teachers/student-resources/research-starters/research-starters-worldwide-deaths-world-war.

"Temporary Protection Poland." *Asylum Information Database*, n.d. https://asylumineurope.org/wp-content/uploads/2013/06/AIDA-PL_Temporary-Protection_2022.pdf.

"Ukrainians in Poland and the War in Ukraine." *CBOS*, October 2024. https://www.cbos.pl/PL/publikacje/public_opinion/2024/10_2024.pdf.

Vulnerability to Trafficking in Persons in the Context of the War in Ukraine: Findings from Poland and Romania, n.d. https://eca.iom.int/sites/g/files/tmzbdl2626/files/documents/2024-09/vulnerability-to-tip_war-in-ukraine_poland-and-romania_august-2024.pdf.

Wlodarczak-Semczuk, Anna, and Justyna Pawlak. "Who Is Poland's next President, Karol Nawrocki?" *Reuters*, June 2, 2025. https://www.reuters.com/world/europe/who-is-polands-next-president-karol-nawrocki-2025-06-02.

PART II

SECURITY AND POLICY

1

Reconceptualizing Intelligence: The Application of Gender-Sensitive Intelligence Strategies in Counter-Radicalization and Amendment of Traditional Intelligence Frameworks

Catherine KERCKHOVE

Abstract: As modern security threats grow more convoluted and integrated into society, intelligence agencies must adopt inclusive strategies to maintain their efficacy in ensuring security. This paper examines the merits of integrating gender-sensitive approaches in counter-radicalization pursuits within intelligence agencies and their frameworks. Drawing on feminist security studies, empirical literature, and case studies, the paper evaluates current practices, the scope of their usage, and possibilities for the future. It concludes with recommendations on the basis that gender is an analytical lens that is essential to intelligence analysis to ensure depth, thoroughness, and legitimacy.

Keywords: Gender- Sensitive, Counter-Radicalization, Feminist Security Studies, Women, Peace and Security (WPS), Violent Extremist Organizations (VEO)

Introduction

As a result of increasingly compounding international security threats, the development of more inclusive and refined intelligence paradigms that harness diverse social insights becomes that much more necessary within intelligence agencies. Among the most underutilized strategies is the incorporation of gender-sensitive approaches into human intelligence (HUMINT) gathering. Traditional intelligence gathering integrates a gender-neutral approach that operates within a masculine and hierarchical framework that overlooks gendered experiences that play crucial roles in radicalization.

Contemporary women play increasing roles in radicalization processes and violent extremism as they are advantageously positioned to take on the role of active terrorists, as well as reducing the impact of violent extremism.[194] Despite this knowledge, the role of women is most often reduced to that of victimhood when in actuality they are facets in supporting, enabling, and operating within violent extremist organizations.[195] Notwithstanding, this evidence of women's crucial role, intelligence agencies have largely, in practice, ignored the Women, Peace, and Security Act (WPS) legislation that recognizes the necessity for integration of women-specific perspectives in intelligence.[196] Meaning, intelligence agencies have displayed unhurried approaches to strategically apply gender disaggregated data or to make significant efforts to utilize gender-sensitive units. This reductive, gender-blind gap in intelligence exposes intelligence agencies to missing vital intelligence and practicing ineffective counter-radicalization. Thus, the implementation of gender-sensitive strategies within intelligence agencies will increase the effectiveness of

---

[194] Ellie Hearne, *"Participants, Enablers, and Preventers: The Roles of Women in Terrorism,"* unpublished paper, December 2009. https://is.muni.cz/el/1423/jaro2010/MVZ203/Gender___Terrorism__BISA__Hearne__Dec_2009.pdf.

[195] Anna-Maria Andreeva et al., *"Assessing Gender Perspectives in Preventing and Countering Violent Extremism Practices,"* International Centre for Counter-Terrorism, November 20, 2024. https://doi.org/10.19165/2024.7214.

[196] Katie Crombe and Erin Moffitt, "*Reassessing Women's Role in Peace and Security in the Middle East*," Middle East Institute, January 31, 2022, https://www.mei.edu/publications/reassessing-womens-role-peace-and-security-middle-east.

intelligence by describing gender specific social dynamics, relationships, and early indications of radicalization that are otherwise excluded by the traditional approaches.

This paper argues that integrating gender-sensitive strategies into intelligence gathering enhances operational effectiveness in counter-radicalization by identifying early warning signs, illuminating hidden social networks, and improving contextual understanding of extremist environments. To examine this, the study will address three central questions: (1) How can gender-sensitive approaches improve intelligence operations in counter-radicalization efforts? (2) What measurable gaps exist in current intelligence practices that such approaches can help bridge? and (3) Where and how have gender-based frameworks already impacted counter-extremism strategies globally?

To explore these questions, the research employs a qualitative methodology, drawing on case studies, policy analyses, and comparative evaluations of intelligence initiatives across various geopolitical contexts. The analysis is grounded in feminist security theory, which challenges traditional power structures in security discourse and emphasizes the importance of incorporating diverse lived experiences — particularly those shaped by gender — into strategic analysis and intelligence work.

Literature Review: Gender- Sensitive Intelligence Approaches

Prior literature in feminist security studies suggests that intelligence strategies remain shaped by masculine assumptions, common in the male-dominated field, which often marginalize or overlook gender-specific analysis.[197] Other scholars suggest that the absence of women within security, in tandem with societal expectations of femininity, produces

[197] Aleksandra Gasztold, "*Widok Podejście Feministyczne W Studiach Nad Bezpieczeństwem*," Amu.edu.pl (University of Warsaw, October 7, 2017), https://pressto.amu.edu.pl/index.php/pp/article/view/10650/10238.

hegemonic masculinity over the intelligence and security fields.[198] Gender, within the context of feminist security studies, transcends everyday meaning to encompass societal structures concerning gender orientation and expectations, the effects of gender on political dynamics, individualized motivations with deference to the polarity between men and women, conflict roles, and organizational structure.[199] Thus, this framework, in itself, suggests the necessity of the incorporation of gender-sensitive thinking in order to address the societal differences among men and women within security questions.

Literature concerning the role of women within extremism is also vital to understanding the context of this research. Women are often thought of as passive participants or victims of violent extremist acts, yet further review reveals a more active mobilization by way of involvement in recruitment, facilitation roles, involvement in logistics, and increasing roles in propaganda campaigns.[200] As the number of women leaving Western nations to join violent extremist organizations (VEOs) outpaces that of men, more attention has been paid to the recruitment tactics of these organizations that have led to this divide. The development of gender-specific propaganda campaigns has allowed VEOs to target untapped demographics, like women, that are statistically more likely to counter-act government opposition. The inclusion of women legitimizes, at least by perception, these groups and increases their effectiveness. Yet, violent extremism is still thought of as a male-dominated phenomenon.[201] In the examples of ISIS activity, the implementation of false narratives of female

---

[198] Eric M. Blanchard, "*Gender, International Relations, and the Development of Feminist Security Theory*," Signs: Journal of Women in Culture and Society 28, no. 4 (June 2003): 1289–1312, https://doi.org/10.1086/368328.

[199] Swati Parashar, "*Gender Matters in Global Politics: A Feminist Introduction to International Relations*," Gender & Development 18, no. 3 (November 2010): 562–65, https://doi.org/10.1080/13552074.2010.521996.

[200] Heather Hurlburt, *"Policy Roundtable: How Gender Affects Conflict and Security," Texas National Security Review*, August 22, 2022. https://tnsr.org/roundtable/policy-roundtable-gender-and-security.

[201] Vikram Kolli, *"Women at the Forefront: A Gendered Lens to Counterterrorism Strategies," Harvard International Review*, September 19, 2024. https://hir.harvard.edu/women-at-the-forefront-a-gendered-lens-to-counterterrorism-strategies.

empowerment serves as an effective recruitment strategy.[202] This contradicts the idea that women's involvement in extremist activities is a result of economic constraints and lack of social equality or mobility, which is indicative of a more traditional gender-blind intelligence understanding. Intelligence practices must follow the evolution of VEO's tactics and recruitment approaches, by way of gender-based analysis, in order to continue combatting their prevalence.

Another important trend within existing literature is that of utilizing women as intelligence assets, specifically within dismantling radicalization pathways. Gender conscious counter-radicalization programs like that of Sisters Against Violent Extremism (SAVE), developed by social scientist Dr. Edit Schlaffer, or Mothers for Life in Nigeria, focus on women's advantageous position within the family in order to counter radicalization efforts.[203] In the case of SAVE, the initiative centers around early detection of radicalization and possible interventions best suited for the position of a mother of a family, demonstrating a family-level approach created on the basis of gender consideration. Mothers for Life is a community-level approach that employs a network of mothers to counter a region-specific threat, the actions and recruitment of Boko Haram. Although not an exhaustive list of examples of gender-based approaches, this demonstrates that consciousness of gender specificity has a place in the development of counter-radicalization efforts.

Policy integration, an operational facet vital to the implementation of this strategy, is also important to recognize within the context of this body. Dating back to 2000, UNSCR 1325, a United Nations Security Council resolution on women, peace, and security, recognized the pervasiveness of gender within all sections of security. Yet, two decades later, agencies across the world have continued to recognize this, yet sideline efforts to fix the mechanisms in place that still expose agencies to vulnerabilities on

---

[202] Elizabeth Weingarten, *"Why Female Extremists Perplex Us," TIME*, March 21, 2015. https://time.com/3751706/female-extremists.

[203] Moussa Bourekba, *Overlooked and Underrated? The Role of Youth and Women in Preventing Violent Extremism*, CIDOB, November 2020, https://www.cidob.org/publicaciones/overlooked-and-underrated-role-youth-and-women-preventing-violent-extremism?ref=hir.harvard.edu.

account of ignorance of gender influence.[204] Therefore, despite this evidence and directive from the Security Council, little meaningful action has been taken in the following years. In addition to this, the United Nations Plan of Action to Prevent Violent Extremism of 2016 goes further to advocate for more gender-sensitive research, exploration of the capacity of this approach, and specific field applications that are gender-sensitive. Special attention must also be paid to using this strategy as an intelligence enhancement rather than a mechanism of further stereotyping.[205]

A summation of the existing literature reveals that gender is not merely a variable that can be overlooked but a central aspect of intelligence gathering and radicalization processes. Under-implementation on the part of intelligence agencies reveals vulnerabilities like the over-dependence on outdated assumptions of women's roles, the absence of operational applications within intelligence agencies, and the continuation of shallow analysis that overlooks gender nuance. As the literature dictates, VEOs integrate women, yet intelligence agencies have yet to comprehensively apply the same principles to counter this development.

Traditional Approach: Structure and Gender-Blind Limitations

Within the traditional structure of intelligence agencies, there is often a bias towards a hierarchical structure that is based on models dominated by men throughout history. This not only affects recruitment and decision-making models but also creates undue skepticism in women's roles within the field, as they are less historically founded. Overlooking these disadvantageous representations and the analytical lens capable of identifying gender specific warning signs. Despite the United States Intelligence Authorization Act of 2022 that recognized this unique opportunity within

[204] Jocelyn Trainer, "Applying a Gender Lens to Security Studies," *The International Affairs Review*, July 12, 2021, https://www.iar-gwu.org/print-archive/ikjtfxf3nmqgd0np1ht10mvkfron6n-bykaf-ey3hc.

[205] Jayne Huckerby, "Gendering Counterterrorism: How To, and How Not to — Part I," *Just Security*, May 2018, https://www.justsecurity.org/55522/gendering-counterterrorism-to.

intelligence and provided directions to the National Security Agency to integrate the approach into tradecraft, implementation remains largely stagnant and incomplete.[206]

Within active methodology, the lack of gender disaggregated data means the loss of the ability to understand and distinguish between demographics and behavioral groups. Meaning, when modeling threats, intelligence operates under gender-blind assumptions that can fail to recognize gender specific intimations. In the modern age that values direct threat assessment through technical means, approaches like rapport building, empathetic considerations, and communication, tactics women analysts excel at, become undervalued assets. Therefore, despite empirical data on emotional intelligence, this strength that women could disproportionately provide remains untapped.[207]

The same U.S. Intelligence Act in 2022 also specifically referenced the ability of women to access populations and social situations that are unreachable by men. This mention, in itself, exposes a gap left unaddressed despite awareness and plausible options to rectify it.[208]

Comparative Case Studies

Two cases where gender-sensitive applications were used directly in an operational capacity are the female engagement teams in Afghanistan and Team Lioness in Iraq, two United States initiatives. Through analysis and comparison, the efficacy of this work can be ascertained, as well as the limitations identified. In Afghanistan in 2009, the US developed a population-focused team, or Female Engagement Team, to address

---

[206] Adam B. Schiff (D-CA-28), "Text — H.R.5412 — 117th Congress (2021–2022): Intelligence Authorization Act for Fiscal Year 2022," *Congress.gov*, 2021, https://www.congress.gov/bill/117th-congress/house-bill/5412/text.

[207] Chara Papoutsi et al., "Emotional Intelligence & ICTs for Women and Equality," *Technium Social Sciences Journal* 27 (January 8, 2022): 253–68, https://doi.org/10.47577/tssj.v27i1.5561.

[208] Adam B. Schiff (D-CA-28), "Text — H.R.5412 — 117th Congress (2021–2022): Intelligence Authorization Act for Fiscal Year 2022," *Congress.gov*, 2021, https://www.congress.gov/bill/117th-congress/house-bill/5412/text.

counter-terrorism through winning regional support. The previously inaccessible demographic, Afghan women, were identified as victims of targeted exploitation by extremists. The cultural sensitivity, surrounding women especially, in the region, prevented male U.S. soldiers from interacting with these women. As a result, they became a common workaround for terrorists and smugglers. FETs became a deterrence strategy against the utilization of women in this capacity, thus creating an increased potential for actionable intelligence as well. FET's which evolved from Lioness teams, grew by 2008 to include the running of medical clinics, distribution of medicine, assistance at checkpoints, and conducting engagements in Afghan homes. The success of such teams is recognized as beneficial in intelligence but has not been optimized because it remains isolated instead of being employed throughout the armed forces with consistent recruitment. Others argue that the nature of their as-needed deployments prevents them from truly being proven effective. Lastly, it was noted that rapport building was successful and led to high-value targets and intelligence, yet their teams were reduced to administrative support, and accountability was low because of the lack of protocol.[209]

The precursor, the Lioness Teams deployed in Iraq, were developed to remain situationally aware and address the cultural sensitivities of the native culture so as not to worsen the perception of United States involvement. After a week-long training, these women would be attached to traditional infantry units and deployed primarily to perform searches on native women. However, these women were often deployed as lone attachments to traditional units, meaning they were not organized into units of their own that worked in conjunction as a group. They are recognized by fellow marines to have provided huge gains in the counterinsurgency realm in which they were tasked to access the inaccessible, like FETs.

Lioness teams became the action that set a precedent for gender-sensitive units to follow. Their demonstrated covert access to women and children as well as the new intelligence gains provided were facets of intelligence that

---

[209] Raymond Kareko, "Female Engagement Teams," *Army University Press*, October 25, 2019, https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2019/October/Female-Engagement-Teams.

were carried on to FETs. This second application in Afghanistan proved that the evolution of gender-based approaches was possible and continued to increase intelligence access, diversify opportunities, and build community trust. However, both were severely limited by the lack of a previous foundation for their work. Lioness teams faced struggles on account of leadership and their willingness to adapt, as well as the largely informal process of their deployment and duties. FETs continued to face weak standardization, logistical issues, and small-scale integration. Further development of gender-based approaches is therefore possible, but it is a necessity to optimize their work first and foremost.[210]

Challenges and Ethical Considerations

This integration of gender-sensitive intelligence practices introduces a number of challenges on the part of ethical considerations, operational hurdles, and cultural concerns. The first ethical consideration is instrumentalization. It is important to remain cautious against creating these programs just to access this new intelligence realm. This risks reinforcing gender stereotypes and overlooking meaningful and productive integration. This becomes especially relevant considering the cessation of both the Lioness teams and FETs.[211] Overlooking the value of true integration results in short-lived benefits, as in the case of these two programs. Gender-sensitive approaches, in order to be sustainable and impactful, will require long-term structural change instead of brief deployments.

Cultural considerations must follow a two-pronged approach. As established, the largely male-dominated field will potentially display internal bias against the implementation of this nature. Gender-sensitivity, in itself, is a method that forces an analyst or operator to think specifically as a member of the subject's in-group would. This contradicts the masculine

---

[210] Nicholas Dunn, "Lioness Program 'Pride' of the Corps," *Marine Corps Air Ground Combat Center Twentynine Palms*, March 13, 2009, https://www.29palms.marines.mil/Articles/Article/498488/lioness-program-pride-of-the-corps.

[211] Raymond Kareko, "*Female Engagement Teams*," *Army University Press*, October 25, 2019, https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2019/October/Female-Engagement-Teams.

intelligence trend the industry is accustomed to. Without the backing of policy reform and increased gender-sensitive education, women enlisted to practice this approach or others advocating on behalf of it may experience pushback. Second, external concerns must also be considered, especially when physically operating within gender-segregated societies. Women operating in this capacity in largely conservative regions may build a negative reputation and inherit mistrust that might endanger the operator. As women's roles increase and involve more locals, there will need to be subsequent development of protection for those at risk of backlash for collaboration with female agents, as well as for the agents themselves.

There must also be a discussion over ethics concerning operations and data. Similar to the protection of privacy, this must be extended to gendered intelligence collection as well to bolster its credibility and justification. Oversight must be utilized as it is in other types of intelligence. This type of intelligence also relies more heavily on human intelligence rather than data, meaning it is that much more important that claims be substantiated and validated so the information does not become untrustworthy on account of assumptions or emotions.

Over-reliance on gender specifically is another possible challenge. Adopting a one-dimensional view of information, or relying only on the perspective of the subject's gender alone, will take away from the subject's other influential factors. Intersectional factors like religious identity, race, class, ethnicity, and sexual orientation must also be considered.

Recommendations

Institutional

With consideration of the evidence presented, there are several substantiated recommendations that would facilitate actionable implementation of gender-sensitive intelligence strategies. The first of which would be leadership-initiated and backed agency-wide reform. This broad recommendation would include specific integration methods like the requirement

of gender-disaggregated data reporting, specific requirements built around accessing gender roles within collected actionable intelligence, and increased education on identifying areas where gender nuance could provide higher quality intelligence. Generally housed under the concept of gender mainstreaming, the intentional integration of gender considerations in all areas of intelligence is advocated for by UN Women.[212] This could include an increased emphasis on endeavoring to understand perspective over perception in differing cultures regarding gender and societal structures, specifically.

If institutional reform of this nature is rejected, an alternate route could be the separation of a more specialized unit trained in gender-sensitive intelligence. Just like the separation between intelligence units dealing with human intelligence versus signal intelligence, another distinction could be made to establish professionals capable of weighing in on any collected intelligence.

Operational

Beyond institutional initiatives, tangible operations changes must also be incorporated by way of FETs, community-led initiatives, and AI implementation. Despite past shortcomings, increased investment in FETs that incorporate changes made from past trials remains a promising security agency possibility. This further investment would allow for the expansion past its previous operational capability, which largely relied on patrols, into a stronger intelligence capacity. Properly educated and utilized FETs deployed within regions that remain largely separated on the basis of gender could be the precipice of new intelligence capabilities.[213] This could also take the form of mixed gender units to more sustainably apply these tactics, especially during times of transition to gender-sensitive approaches.

---

[212] Jacqui True, "How Effective Is Gender Mainstreaming in International Peace and Security Policymaking?" (Monash University; Edward Elgar Publishing, 2016), https://research.monash.edu/en/publications/how-effective-is-gender-mainstreaming-in-international-peace-and-.

[213] Gina Jones, *Female Engagement Teams: Making the Case for Institutionalization Based on U.S. Security Objectives in Africa: A Monograph* (Defense Technical Information Center; Defense Intelligence Agency, May 23, 2013), https://apps.dtic.mil/sti/citations/ADA583961.

As seen by the successful application of gender perspectives in organizations like Mothers for Life or SAVE, community-focused initiatives are among the most promising. Partnership with regionally effective non-governmental organizations, especially those run by women for women, to cooperate on community-based programs. This local focus serves as a mechanism to create more personal and lasting change, with an additional benefit of building trust in the intelligence community, which allows for more free-flowing information. Creating bilateral trust would enable intelligence agencies to implement training for women specifically to serve in an early detection capacity.[214]

Lastly, increased data collection that is gender-sensitive is another application needed within the intelligence field. Investment in artificial intelligence capabilities that employ a component of gender-specific recognition capabilities, especially in the form of You Only Look Once (YOLO) applications or other tools capable of examining large collections of data efficiently. This would allow for data collection that is specific to the variable of gender and allow further research to be done, more empirically, on gender specific threat signals.[215] Where grassroots community-level approaches could address real-time radicalization efforts done on a person-to-person level, AI capabilities could address online radicalization efforts quicker by data analysis and flagging than a human noticing new radicalization patterns.

Policy

To ensure the safety and maintenance of this application, policy reform must also be developed. The Organization for Security and Co-operation in Europe (OSCE) calls for oversight policy codified into security law that monitors integration and ensures proper training and protocol evaluation. This would also include safeguards for those involved directly in programs.

---

[214] Adam B. Schiff (D-CA-28), "Text — H.R.5412 — 117th Congress (2021–2022): Intelligence Authorization Act for Fiscal Year 2022," *Congress.gov*, 2021, https://www.congress.gov/bill/117th-congress/house-bill/5412/text.

[215] Clarisa Nelu, "*Harnessing AI for Online P/CVE Efforts: Tools, Challenges, and Ethical Considerations,*" *Global Network on Extremism and Technology*, February 24, 2025, https://gnet-research.org/2025/02/24/harnessing-ai-for-online-p-cve-efforts-tools-challenges-and-ethical-considerations.

This means the development of protection mechanisms that create protection protocols, have operational capabilities to respond to emergencies, and have some capacity for support after service.[216]

Conclusion

The growing complexity of global security threats like ideological radicalization and violent extremism creates a need for transformation in methodology and conceptualization within intelligence. Integrating gender-sensitive approaches into the intelligence, counter-radicalization, and counter-insurgency frameworks is a necessity rather than just a symbolic act of inclusion. It is now understood that women are not only targets or victims of extremism but are capable of being both active participants and active counterforces. Disregarding the role of gender-based approaches creates space for incomplete and ineffective intelligence that undermines counter-radicalization work.

The long-standing gender-blind approach, stemming from masculine philosophy and structure, does not account for social nuance or differentiated warning signals that can denote extremist actions. This omission is exacerbated by intelligence agencies continuing to delay or procrastinate meaningful implementation of suggestions made by various global security acts like UN Security Council Resolution 1325 or the United States Intelligence Authorization Act of 2022 that advocate for more significant involvement of women in peace and security efforts. Previous operational capabilities like Lioness or Female Engagement Teams provide proof of concept, yet their impacts are still limited by the extent and nature of their usage thus far. Their limitations provide evidence as to why structural reform needs to take place to address the inconsistencies that dampened their effects.

Intentional planning, local engagement, and detailed structure of oversight must be utilized to address ethical and cultural concerns that may

[216] Henri Myrttinen, *Security Sector Governance, Security Sector Reform and Gender* (Geneva: Geneva Centre for Security Sector Governance (DCAF), 2019), https://www.osce.org/files/f/documents/1/1/440834_0.pdf.

arise in response to the application of gender considerations. Internal bias and resistance can be dealt with through top-down approaches of leadership-backed mandates as well as the introduction of robust AI applications attuned to gender differences within counter-radicalization.

Gender-blind intelligence could be considered a framework from the past, while effective intelligence, especially counter-radicalization efforts, of the future becomes increasingly cognizant of gender-sensitive intelligence approaches. Agencies must arm themselves with the capabilities to recognize gender as more than an outside variable but as an important facet for understanding specific human behavior and patterns of thinking. A gender-sensitive approach to counter-radicalization offers enhanced analytical and operational capacity within the intelligence community to better safeguard and protect their respective nations' security and interests. Moving forward, more research is needed to fully understand and harness the possibilities of gender-sensitive intelligence operations.

Bibliography

Andreeva, Anna-Maria, Annika von Berg, Bibi van Ginkel, Elisabeth Hell, Shams Jouve, Alexandra Korn, Bàrbara Molas, Maximilian Ruf, and Sophie Scheuble. *Assessing Gender Perspectives in Preventing and Countering Violent Extremism Practices*. The Hague: International Centre for Counter-Terrorism, November 20, 2024. https://doi.org/10.19165/2024.7214.

Blanchard, Eric M. "Gender, International Relations, and the Development of Feminist Security Theory." *Signs: Journal of Women in Culture and Society* 28, no. 4 (June 2003): 1289–1312. https://doi.org/10.1086/368328.

Bourekba, Moussa. "Overlooked and Underrated? The Role of Youth and Women in Preventing Violent Extremism." CIDOB, November 2020. https://www.cidob.org/publicaciones/overlooked-and-underrated-role-youth-and-women-preventing-violent-extremism?ref=hir.harvard.edu.

Crombe, Katie, and Erin Moffitt. "Reassessing Women's Role in Peace and Security in the Middle East." *Middle East Institute*, January 31, 2022. https://www.mei.edu/publications/reassessing-womens-role-peace-and-security-middle-east.

Dunn, Nicholas. "Lioness Program 'Pride' of the Corps." *Marine Corps Air Ground Combat Center Twentynine Palms*, March 13, 2009. https://www.29palms.marines.mil/Articles/Article/498488/lioness-program-pride-of-the-corps.

Gasztold, Aleksandra. "Podejście Feministyczne w Studiach nad Bezpieczeństwem." *Przegląd Politologiczny* 4 (2017): 135–147. https://pressto.amu.edu.pl/index.php/pp/article/view/10650/10238.

Hearne, Ellie. "Participants, Enablers, and Preventers: The Roles of Women in Terrorism." Paper presented at the British International Studies Association Annual Conference, December 2009. https://is.muni.cz/el/1423/jaro2010/MVZ203/Gender___Terrorism__BISA__Hearne__Dec_2009.pdf.

Huckerby, Jayne. "Gendering Counterterrorism: How To, and How Not to – Part I." *Just Security*, May 2018. https://www.justsecurity.org/55522/gendering-counterterrorism-to.

Hurlburt, Heather. "Policy Roundtable: How Gender Affects Conflict and Security." *Texas National Security Review*, August 22, 2022. https://tnsr.org/roundtable/policy-roundtable-gender-and-security.

Jones, Gina. *Female Engagement Teams: Making the Case for Institutionalization Based on U.S. Security Objectives in Africa: A Monograph*. Defense Technical Information Center. Defense Intelligence Agency, May 23, 2013. https://apps.dtic.mil/sti/citations/ADA583961.

Kareko, Raymond. "Female Engagement Teams." *Army University Press*, October 25, 2019. https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2019/October/Female-Engagement-Teams.

Kolli, Vikram. "Women at the Forefront: A Gendered Lens to Counterterrorism Strategies." *Harvard International Review*, September 19, 2024. https://hir.harvard.edu/women-at-the-forefront-a-gendered-lens-to-counterterrorism-strategies.

Myrttinen, Henri. *Security Sector Governance, Security Sector Reform and Gender*. Geneva: Geneva Centre for Security Sector Governance (DCAF), 2019. https://www.osce.org/files/f/documents/1/1/440834_0.pdf.

Nelu, Clarisa. "Harnessing AI for Online P/CVE Efforts: Tools, Challenges, and Ethical Considerations." *Global Network on Extremism and Technology*, February 24, 2025. https://gnet-research.org/2025/02/24/harnessing-ai-for-online-p-cve-efforts-tools-challenges-and-ethical-considerations.

Papoutsi, Chara, Irene Chaidi, Athanasios Drigas, Charalabos Skianis, and Charalampos Karagiannidis. "Emotional Intelligence & ICTs for Women and Equality." *Technium Social Sciences Journal* 27 (January 8, 2022): 253–68. https://doi.org/10.47577/tssj.v27i1.5561.

Parashar, Swati. "Gender Matters in Global Politics: A Feminist Introduction to International Relations." *Gender & Development* 18, no. 3 (November 2010): 562–65. https://doi.org/10.1080/13552074.2010.521996.

Trainer, Jocelyn. "Applying a Gender Lens to Security Studies." *International Affairs Review*, July 12, 2021. https://www.iar-gwu.org/print-archive/ikjtfxf3nmqgd0np1ht10mvkfron6n-bykaf-ey3hc.

True, Jacqui. "How Effective Is Gender Mainstreaming in International Peace and Security Policymaking?" Monash University. Edward Elgar Publishing, 2016. https://research.monash.edu/en/publications/how-effective-is-gender-mainstreaming-in-international-peace-and-.

U.S. Congress. House. *Intelligence Authorization Act for Fiscal Year 2022*. H.R. 5412, 117th Congress, 1st sess., 2021. https://www.congress.gov/bill/117th-congress/house-bill/5412/text.

Weingarten, Elizabeth. "Why Female Extremists Perplex Us." *TIME*, March 21, 2015. https://time.com/3751706/female-extremists.

2

Challenges of Security: Questions of Domestic Surveillance & Privacy Rights in the United States

Ashlyn MUNDELL

Abstract: Following the terrorist attack on September 11, 2001, the function of domestic surveillance in the United States shifted drastically. Apprehensions of successive attacks became a guise under which surveillance morphed into an instrument of those in positions of political and social power. This paper explores the domestic surveillance policy in the United States post-9/11 and its violation of the privacy rights of citizens. After critically analyzing both EU and US surveillance policy, alongside deconstructions of programs like XKeyscore, PRISM, and COINTELPRO, this paper identifies clear patterns of governmental overreach continuously masked as counterterrorism. In addition, this paper explores the consequences of unethical surveillance, including discussions on hegemonic social stratification, generalized interpersonal ramifications, and the chilling effect in relations to democratic participation. Conclusively, this paper proposes US policy recommendations modeled after EU domestic surveillance frameworks, namely the GDPR and the ECHR.

Keywords: Domestic surveillance, chilling effect, privacy rights, security, counterterrorism

Introduction

Domestic surveillance has become a central pillar of U.S. national security policy, particularly in the aftermath of the September 11, 2001 attacks. Legislative expansions such as the USA PATRIOT Act and subsequent intelligence reforms have significantly broadened the scope of government surveillance, enabling unprecedented monitoring of both citizens and non-citizens. While these policies are justified by the state as essential to counterterrorism efforts, critics argue they compromise civil liberties — especially the constitutional right to privacy.

This paper examines whether and how post-9/11 domestic surveillance practices — both legal and extralegal — violate U.S. citizens' right to privacy. Drawing on secondary literature, case law, policy analysis, and existing critiques, it explores the ethical and social consequences of unchecked surveillance, with a particular focus on its role in reinforcing structural inequalities and suppressing democratic participation through the "chilling effect." The paper also engages in a comparative analysis of domestic surveillance policies in the European Union to formulate policy recommendations aimed at reducing harm while preserving national security.

Key concepts such as *domestic surveillance*, *illegal surveillance*, and the *chilling effect* are clarified to provide a shared analytic framework. Domestic surveillance and illegal domestic surveillance, while sharing several components, are vastly different. Domestic surveillance is the gathering of information on a nation's homeland conducted by that nation's coercive agencies, such as the police.[217] What can make domestic surveillance illegal is when those agencies overstep their limits in regard to what they can or cannot document and they disregard any outlined justifications for that monitoring.[218] Also relevant is the chilling effect. This term describes the phenomena in which participation in basic democratic functions and the

[217] Jeffrey Ian Ross and David O. Friedrichs, "Illegal Domestic Surveillance," in *An Introduction to Political Crime*, 1st ed. (Bristol University Press, 2012), 101–14, https://doi.org/10.2307/j.ctt1t898f9.

[218] Ross and Friedrichs, "Illegal Domestic Surveillance," 101–14.

expression of personal ideologies by an individual are muted as a result of otherwise intimidating or confusing policymaking.[219]

Ultimately, the paper argues that current U.S. surveillance practices disproportionately target marginalized communities, erode democratic norms, and require urgent policy reform — particularly through models inspired by EU frameworks that emphasize transparency, accountability, and citizen rights. In the proceeding sections, this paper first looks at the US legal framework post 9/11, their social implications, and concludes by providing policy recommendations.

U.S. Legal Frameworks Post 9/11

After 9/11, domestic policy regarding surveillance focused heavily on fighting both realities and imagined threats of terrorism. President George W. Bush, for example, sanctioned the "Authorization for the Use of Military Force (AUMF)" in 2001 in response to the attack.[220] This order gave the National Security Agency permission to conduct counterterrorism surveillance where deemed necessary or appropriate *without* a warrant.[221] The PATRIOT Act, which was passed the following October, was designed to allow law enforcement agencies to use various heightened levels of surveillance on a wider range of criminal acts in an effort to counter terrorism.[222] This also permitted many federal actors a broader range of authorizations in surveilling anything considered a threat to Americans both domestically or abroad. Furthermore, the sharing of intelligence between government agencies for investigative purposes was sanctioned.[223] In short, the PATRIOT Act and AUMF were designed to fight the war on terror on U.S. soil but

---

[219] "The Establishment Clause and the Chilling Effect," *Harvard Law Review* 133, no. 4 (February 10, 2020), https://harvardlawreview.org/print/vol-133/the-establishment-clause-and-the-chilling-effect.

[220] Michael T. Martínez et al., "Press Narratives of NSA Domestic Surveillance," *Atlantic Journal of Communication* 28, no. 2 (2020): 86, https://doi.org/10.1080/15456870.2020.1709462.

[221] Martínez et al., "Press Narratives of NSA," 85–102.

[222] U.S. Department of Justice, *The USA Patriot Act: Preserving Life and Liberty* (2001), https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

[223] U.S. Department of Justice, *The USA Patriot Act*, 2001.

also signaled a tone shift in policymaking involving privacy rights for the average citizen.

As intelligence agencies gained expanded authority to surveil individuals on U.S. soil, the boundaries of who could be monitored — and how and why — quickly became blurred.

Domestic surveillance efforts initially justified as counterterrorism tools, increasing become a convenient way to monitor U.S. citizens — a practice that, in our tech-saturated age, often amounts to a direct assault on personal privacy. While most initiatives, programs, and actors involved in national spying follow outlined legislative procedures to ensure individual rights remain protected, there remains a lack of regulations on operations not immediately visible to the public. Fundamentally, illegal domestic surveillance is distinguishable from legitimate surveillance because it exhibits characteristics inherently unconstitutional such as opening mail, placing listening devices in private properties, and wiretapping.[224] The key similarity is that both legal and illegal domestic surveillance are exclusively conducted by state actors including but not limited to the military, current administrations, police, and federal agencies. This style of security practices inherently makes those observed uncomfortable when unconcealed, so it is natural for the agencies involved to veil any programs that may create distrust and unease in the public. The NSA, for example, was sanctioned by the PATRIOT Act, to monitoring any and all communications in the U.S. without any appropriate mandates.[225]

However, this paper maintains that prior to 9/11, government agencies were already heavily involved in illegal domestic surveillance. To serve as a powerful illustration, the CIA ran an operation titled Project Resistance, designed to study and monitor dissidence groups on college campuses.[226]

---

[224] Ross and Friedrichs, "Illegal Domestic Surveillance," 101–14.

[225] David Sauer, "Domestic Surveillance in the United States" (briefing paper, Harvard Model Congress, 2025), https://static1.squarespace.com/static/5cb7e5637d0c9145fa68863e/t/6729677bc8c13f0fbc586e93/1730766716640/House+Intelligence+-+Domestic+Surveillance.pdf.

[226] John Prados, "Domestic Surveillance," in *The Family Jewels: The CIA, Secrecy, and Presidential Power* (Austin: University of Texas Press, 2014), 35–64.

This operation was responsible for the creation of over six hundred files on American citizens purely for their political affiliations. In addition, over twelve thousand or more individuals' names were noted for similar reasons. This program exemplifies the tendency of secret domestic surveillance operations to be invasive, prejudiced, and politically motivated.

The secretive nature of many government surveillance operations often conceals misconduct from the public eye. This was made starkly evident in 2013, when Edward Snowden exposed the National Security Agency's (NSA) surveillance practices, revealing a system that closely resembled a 'surveillance state.' One of the first revelations involved the NSA collecting communication and call data from Verizon users — a practice justified as counterterrorism by the Foreign Intelligence Surveillance Court.[227]

Under growing public scrutiny, the NSA's Project Prism was quickly unsurfaced to reveal even further unwarranted surveillance of Americans by their own government. This post-9/11 program allowed the NSA to access user data from major internet companies such as Apple and Google, including search history, email content, chats and files.[228] Alarmingly, these companies complied with the requests, often without significant protest. While national security and counterterrorism are legitimate concerns, these justifications clearly eclipsed moral and ethical boundaries — both within government institutions and among corporate partners.

Snowden's whistleblowing extended beyond PRISM. He also exposed XKeyscore, another domestic electronic surveillance operation. Unlike PRISM's targeted data collection, XKeyscore allowed for a broader range of surveillance — tracking nearly everything a typical user does online.[229] According to reports published after Snowden's disclosures, the program captured the content of emails, visited websites, search queries, and metadata.

---

[227] Michael Register, Justifying the Means: Electronic Domestic Surveillance Programs before and Following the September 11, 2001, Terrorist Attack on the United States (PhD diss., Utica College, 2016).

[228] Register, "Justifying the Means," 2016.

[229] Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'" *The Guardian*, July 31, 2013, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Analysts could sift through this data using identifiers like names, phone numbers, IP addresses, and keywords, raising serious concerns about privacy and unchecked surveillance capabilities.[230]

Fearing governmental retaliation, Snowden fled to Hong Kong in 2013[231] and later received asylum in Russia.[232] His actions underscore a disturbing reality: more than a decade after 9/11, the United States government continues to exploit the rhetoric of security and counterterrorism to justify invasive surveillance. Had Snowden not acted, would Prism and XKeyscore still be operating in the same capacities today? And how many similar programs remain active, hidden from public scrutiny?

While domestic surveillance can serve legitimate national security purposes, its abuse — and the punishment of those who try to expose it — demands a closer look at the integrity of both policy and policymakers. When rectifying wrongdoing is met with exile, the moral compass of those in power must be seriously questioned.

It is also important to acknowledge that overreaching domestic surveillance is not a phenomenon born from the post- 9/11 era — nor exclusive to modern U.S. intelligence practices. In fact, leaked documents and investigative reports have revealed that the government engaged in aggressive surveillance tactics well before 2001. One of the most notorious examples is COINTELPRO, the FBI's Counterintelligence Program, which ran from the mid-50's to the early 70's.

COINTELPRO was designed to monitor, infiltrate, and disrupt a range of dissident groups, including the Black Panthers, the American Indian Movement, and the Communist Party of the U.S. — actions justified under the broad malleable label of political extremism.[233] Disturbingly, the program's reach went beyond organized groups. One document

---

[230] Register, "Justifying the Means," 2016.

[231] Ibid.

[232] Andrei Soshnikov et al., "NSA Whistleblower Edward Snowden Is Now a Registered Russian Taxpayer, RFE/RL Finds," *RadioFreeEurope/RadioLiberty*, May 30, 2025, https://www.rferl.org/a/russia-snowden-nsa-whistleblower-taxpayer/33429552.html.

[233] Ross and Friedrichs, "Illegal Domestic Surveillance," 107.

revealed that the daughter of a sitting congressman was listed as a national security concern simply for publicly opposing the Vietnam war. This level of surveillance suggests that the FBI showed little concern for ethical boundaries — or even plausible justification — when determining who could be targeted.[234]

This historical context serves to emphasize a critical point: illicit domestic surveillance has long embedded in the operations of the United States security state. The events of 9/11 did not create this reality; they simply shifted its tone, intensity, and public justification. In many ways, 9/11 functioned as a modulation point — a moment that redefined what "national security" meant and dramatically expanded the powers granted in its name.

Social Implications

Hegemonic Social Stratification

Improperly executed domestic surveillance carries significant consequences — both intended and unintended — that reverberate throughout society. Two major outcomes often emerge: the reinforcement of existing social hierarchies and the erosion of civil liberties. Illegitimate surveillance, whether through programs resembling XKeyscore, PRISM, or COINTELPRO, tends to serve the interests of dominant social and political groups. In doing so, it reinforces hegemonic structures by targeting marginalized or dissenting voices under the guise of maintaining national security.

This dynamic raises a pressing question: should the protection of national security consistently supersede democratic norms and constitutional rights? While some argue that security must take precedence, this line of thinking blurs the boundary between justified vigilance and authoritarian overreach. Ultimately, it forces a critical reckoning — where should

[234] James Kirkpatrick Davis, Spying on America: The FBI's Domestic Counterintelligence Program (Bloomsbury Publishing USA, 1992).

society draw the line between what constitutes a legitimate threat and what amounts to a dangerous breach of personal freedom?

Unwarranted public surveillance poses as a threat to democratic functions on a national level.[235] Public perceptions of governmental power, checks, and balances often directly reflect the quality of a functioning democracy. When dissent and protest are met with covert surveillance — such as intelligence-gathering at demonstrations — it sends a clear message: opposition is unacceptable. This not only undermines First Amendment protections but also creates a chilling effect that discourages civic participation.[236]

Raphael Schlembach, in his analysis of undercover policing, argues that "the covert policing of protest is not designed to detect and prevent crime; it is to *fabricate and maintain order*."[237] This perspective casts domestic surveillance in a troubling light — one that prioritizes control over justice. The issue becomes even more invasive when surveillance enters private spaces. Remote tactics such as electronic bugging or off-site access to household electronics, are rarely justifiable as anything other than displays of unchecked governmental power.[238] While often rationalized as counterterrorism measures, such intrusions blur — or outright violate — constitutional boundaries, particularly those established by the First and Fourth Amendments.

At its core, extremist domestic surveillance is a tool for maintaining power — not safety. When a government engages in such practices, it signals a fundamental shift: power is no longer shared or checked, but hoarded by those behind the surveillance apparatus. The cost is not just privacy, but also dignity, autonomy, and even identity. Stripped of the right to control

---

[235] Sunny Skye Hughes, "US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program," *Canadian Journal of Law & Society/Revue Canadienne Droit et Societe* 27, no. 3 (2012): 399–425.

[236] Hughes, "US Domestic Surveillance after 9/11," 399–425.

[237] Raphael Schlembach, "Undercover Policing and the Spectre of 'Domestic Extremism': The Covert Surveillance of Environmental Activism in Britain," *Social Movement Studies* 17, no. 5 (2018): 491–506.

[238] Sophia Maalsen and Jathan Sadowski, "The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance," *Surveillance & Society* 17, no. 1/2 (2019): 118–24.

one's own information, individuals lose the very conditions that make democratic participation — and personhood — possible. Surveillance, in this context, becomes more than a tactic; it becomes a mechanism of control that undermines the very freedoms it claims to protect.

Interpersonal Ramifications

Beyond its role as a tool of hegemonic control, illegal or unethical surveillance carries broader consequences for the social cohesion and fluid functioning of a society — especially in a nation as diverse as the United States. One of the most significant effects is the creation of the chilling effect, where individuals censor their own behavior in fear of surveillance or government retaliation.[239] While the theory is often framed in terms of verbal or written expression, the concept of 'communication' should be expanded further. People communicate not just through speech or text, but also communicate through their attire, social media presence, group affiliations, and even their general public presence.

When individuals suspect that their actions or affiliations may be interpreted as politically subversive or contrary to prevailing policy, they may choose to hide or suppress aspects of their identity and beliefs. Sunny Skye Hughes explains, even the perception of being monitored — such as during a private phone conversation — can discourage participation in the "marketplace of ideas." She argues that individuals may self-sensor simply because they fear punishment for expressing politically unpopular or legally grey viewpoints, regardless of whether any laws are actually broken.[240] In this way, unethical surveillance doesn't just control actions; it fundamentally alters how people exist and express themselves within society.

Intention plays a key role in both the emergence of the chilling effect and the extent to which it impacts everyday citizens. While public reactions to policy are often beyond direct government control; ethical boundaries are

[239] Hughes, "US Domestic Surveillance after 9/11," 399–425.

[240] Ibid., 400.

clearly crossed when a governing body intentionally weaponizes surveillance to silence, alter, or dismantle disagreeable socio-political groups.[241] In such cases, mass surveillance shifts from a tool of security to a calculated instrument of manipulation and discrimination.

What makes the shift particularly dangerous is the malleability of the terms like 'necessary.' In the case of national security, nearly any action can be framed as necessary if the facts are selectively presented or manipulated. While some rationalizations for targeting specific social groups may be given superficial legitimacy, the risks posed of unchecked, opaque surveillance practices consistently outweigh the potential benefits.

More broadly, the chilling effect not only highlights the effectiveness of domestic spying as a tool for social control, but also demonstrates the capacity of government to forcibly oppress those who do not conform to dominant ideologies. In addition, irregular surveillance may promote prejudice in U.S. criminal justice and security networks. Entire communities — defined by nationality, religion, or race — can be cast as an inherent threats to national security, resulting in widespread surveillance based on identity rather than evidence. Just as troubling is the social backlash this creates: discriminatory surveillance policies can normalize nationalist and racist attitudes among those not targeted, deepening societal divisions and reinforcing systems of power and exclusion.

Policy Recommendations

The following section outlines key domestic surveillance policies implemented in various EU countries. These examples will serve as points of comparison with existing legal frameworks in the U.S. context. It is important to acknowledge that while definitions of privacy, surveillance, and security may vary across cultural and national boundaries, the underlying practice of domestic surveillance — preserving national security — remains largely consistent across democratic states.

---

[241] Hughes, "US Domestic Surveillance after 9/11," 399–425.

To begin, the European Convention of Human Rights specifically outlines privacy as a protected human right,[242] something the U.S. Constitution notably does not.[243] While some argue that privacy rights are implied in First, Third, and Fourth Amendments — protecting religion, the home, the person, and personal property — these provisions were originally designed to address specific, now-outdated threats to the individual, such quartering soldiers in private residences.[244] They offer limited protection against modern threats like massive data collection and pervasive digital surveillance.

What's more, in the United States, privacy rights have largely been shaped through court rulings rather than concrete legislation. The absence of comprehensive federal policy leaves privacy protections fragmented and often outdated — especially in an era defined by rapid technological advancement. In contrast, Article 8 of the ECHR clearly states: "Everyone has the right to respect for his private and family life, his home and his correspondence."[245] It is also outlines strict conditions under which these rights can be lawfully infringed — only in cases justified by national security, public safety, or economic necessity.[246]

This contrast highlights a crucial gap in the American legal doctrine. At the very least, the U.S. Constitution — considered the supreme law of the land — should be amended to explicitly guarantee the right to personal privacy. Such protections must reflect the realities of the digital age, encompassing not only the home and possessions but also personal relationships, affiliations, and digital communications — just as EU policy has moved to do.

---

[242] Alex Stedmon and Glyn Lawson, "Ethical Issues in Surveillance and Privacy," in *Hostile Intent and Counter-Terrorism: Human Factors Theory and Application* (Surrey: Crc Press, 2015).

[243] Douglas Linder, "The Right of Privacy," *Exploring Constitutional Conflicts*, n.d., https://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

[244] Linder, "The Right of Privacy."

[245] European Union Agency for Fundamental Rights, "European Convention on Human Rights — Article 8," European Union Agency for Fundamental Rights, October 25, 2018, https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0.

[246] Council of Europe, "European Convention on Human Rights — Article 8," *European Union Agency for Fundamental Rights*, last updated October 25, 2018, https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0.

The EU has also made extensive progress in establishing policies and procedures intended solely to protect the digital privacy of their citizens — a sharp contrast to surveillance legislation in the U.S. The European Union's General Data Protection Regulation (GDPR) is one of the most vast and comprehensive legal frameworks regarding privacy regulations. This policy was specifically designed with the rapid, modern progression of technology and digital information in mind as it focuses heavily on data privacy, consent, and the right to erase digital material.[31] There is significant emphasis on stricter requirements for consent and the right to 'be forgotten' online; these provisions model ethical policy reform that the United States should seek to replicate domestically.

This is not to say that the United States has not made any effort in policymaking to safeguard individual privacy rights. The Freedom Act of 2015 was designed to respond to the popular concerns and upset that stemmed from the overstep of the PATRIOT Act post 9/11.[32] It should be noted that this corrective measure was introduced over ten years after the original statute — an excessively delayed response to the need for privacy protections in the United States. The act itself limits bulk data collection and enhances digital privacy transparency. Although intended to safeguard privacy rights, the revisions arguably only undid the domestic surveillance powers given to the U.S. government post-9/11 under the PATRIOT Act and do not create any otherwise new protections for citizens.

Conclusion

Domestic surveillance policy has and does undeniably influence the structure of American democracy, often reinforcing existing hierarchies by reshaping how different social, political, and demographic groups are monitored and governed. At the heart of this issue is the urgent need to protect privacy in all its forms — especially as emerging technologies create new vulnerabilities that outdated laws fail to address.

While the sweeping surveillance measures enacted after 9/11 were, in some cases, arguably necessary to protect national security, necessity

must never become a blank check for unchecked power. One traumatic event cannot justify two decades of escalating overreach and erosion of civil liberties. If the U.S. is to uphold its democratic ideals, it must prioritize legal reforms that balance national security with the fundamental rights of its citizens — chief among them, the right to privacy.

From Snowden's whistleblowing to the existence of operations like COINTELPRO, counterterrorism has repeatedly served as a justification for unchecked governmental overreach. Many of the initiatives and programs discussed in this paper would have gone unchecked had it not been for their unintentional revelations to the public where they faced backlash extensive enough to call for their dismantlement. Yet even as these revelations drew scrutiny, U.S. privacy protections have remained outdated — struggling to keep pace with rapidly evolving technologies.

In contrast, the EU has taken a clearer and more proactive approach. Frameworks like the GDPR and ECHR offer a foundation that U.S. policymakers would be wise to study and replicate. Meaningful reforms at the federal level is not only possible — it's necessary. Privacy rights and national security practices can coexist if subjected to necessary deliberation. If left disregarded, the social implications are extensive; toxic nationalism and racism will be stoked, the relationship between the government and the public will falter, and the hegemony will thrive.

Bibliography

Council of Europe. *European Convention on Human Rights*, Article 8. Accessed October 25, 2018. https://fra.europa.eu/en/law-reference/european-convention-human-rights-article-8-0.

Greenwald, Glenn. "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet.'" *The Guardian*, July 31, 2013. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

Hughes, Sunny Skye. "US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program." *Canadian Journal of Law & Society/Revue Canadienne Droit et Societe* 27, no. 3 (2012): 399–425.

James Kirkpatrick Davis. Spying on America: The FBI's Domestic Counterintelligence Program. Bloomsbury Publishing USA, 1992.

Linder, Douglas. "The Right of Privacy." *Exploring Constitutional Conflicts*. Accessed July 9, 2025. https://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html.

Maalsen, Sophia, and Jathan Sadowski. "The Smart Home on FIRE: Amplifying and Accelerating Domestic Surveillance." *Surveillance & Society* 17, no. 1/2 (2019): 118–24.

Martínez, Michael T., Jamie Greig, Catherine A. Luther, and John Baker. 2020. "Press Narratives of NSA Domestic Surveillance." *Atlantic Journal of Communication* 28 (2): 85–102. https://doi.org/10.1080/15456870.2020.1709462.

Prados, John. "Domestic Surveillance." In *The Family Jewels: The CIA, Secrecy, and Presidential Power*, 35–64. Austin: University of Texas Press, 2014.

Register, Michael. "Justifying the Means: Electronic Domestic Surveillance Programs before and Following the September 11, 2001 Terrorist Attack on the United States." PhD diss., Utica College, 2016.

Ross, Jeffrey Ian, and David O. Friedrichs. "Illegal Domestic Surveillance." In *An Introduction to Political Crime*, 101–14. 1st ed. Bristol: Bristol University Press, 2012. https://doi.org/10.2307/j.ctt1t898f9.15.

Sauer, David. "Domestic Surveillance in the United States." *Harvard Model Congress*, 2025. https://static1.squarespace.com/static/5cb7e5637d0c9145fa68863e/t/6729677bc8c13f0fbc586e93/1730766716640/House+Intelligence+-+Domestic+Surveillance.pdf.

Schlembach, Raphael. "Undercover Policing and the Spectre of 'Domestic Extremism': The Covert Surveillance of Environmental Activism in Britain." *Social Movement Studies* 17, no. 5 (2018): 491–506.

Soshnikov, Andrei, Sergei Dobrynin, Yelizaveta Surnacheva, and Dmitry Sukharev. "NSA Whistleblower Edward Snowden Is Now a Registered Russian Taxpayer, RFE/RL Finds." *RadioFreeEurope/RadioLiberty*, May 30, 2025. https://www.rferl.org/a/russia-snowden-nsa-whistleblower-taxpayer/33429552.html.

Stedmon, Alex, and Glyn Lawson. "Ethical Issues in Surveillance and Privacy." In *Hostile Intent and Counter-Terrorism: Human Factors Theory and Application*. Surrey: Crc Press, 2015.

"The Establishment Clause and the Chilling Effect." *Harvard Law Review* 133, no. 4 (February 10, 2020). https://harvardlawreview.org/print/vol-133/the-establishment-clause-and-the-chilling-effect.

U.S. Department of Justice. *The USA Patriot Act: Preserving Life and Liberty*. Washington, D.C., 2001. https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf.

Wheatley, Mary Christine. "Ethics of Surveillance Technologies: Balancing Privacy and Security in a Digital Age." *Premier Journal of Data Science*, November 4, 2024, 1–8. https://doi.org/10.70389/PJDS.100001.

3

French Counterterrorism Operations and Strategic Withdrawal from the Sahel: The Case of Operation Barkhane in Mali

Parker BOURNS

Abstract: In 2013, the French expanded its counter-terrorism efforts in the Sahel through Operation Serval and later Operation Barkhane. By 2022, however, the host governments had requested the withdrawal of French forces. This paper argues that France's military decisions in Mali directly contributed to the formation of the Alliance of Sahel States (AES) and a broader rejection if French influence in the region. Drawing on the case study of French operations in Mali, the analysis explores the implications of this strategic fallout for future relations between the West and its former colonies in the Sahel.

Keywords: Sahel, Operation Barkhane, terrorism, Alliance of Sahel States

Introduction

In the last decade, the Sahel has emerged as a region of growing geopolitical and strategic importance. Since 2011, the Sahel has seen a significant increase in Western military presence and financial assistance.[247] France's

[247] Cécile Berger, *What Role for NATO in the Sahel?* (Rome: NATO Defense College, 2021).

2013 intervention in the Sahel was driven by efforts to suppress terrorist networks and reestablish regional security.

Terrorism is defined in this paper as "an individual or collective enterprise whose objective is to gravely disrupt public order through intimidation and terror."[248]

A significant portion of the terrorist activity in the Sahel, however, has been carried out by groups adhering to jihadist ideologies. Jihadism, as defined by the European Parliament, is "a violent ideology exploiting traditional Islamic concepts. Jihadists legitimize the use of violence with a reference to the classical Islamic doctrine on jihad, a term which literally means 'striving' or 'exertion,' but in Islamic law is treated as religiously sanctioned warfare."[249] This paper adopts that definition as a foundation for analyzing the rise of jihadist groups in the Sahel.

At the start of the Operation Barkhane in 2014, the French were incredibly successful, pushing back the Jihadist terrorists within weeks of being deployed. However, this changed as they attempted to expand the mission. By 2022, the French military and business presence in the Sahel had been pushed out as regional governments reassessed their partnerships. Russia and extremist groups like Boko Haram, ISIS, and JNIM have increasingly moved to occupy the political and security vacuum left by France's withdrawal.[250]

This paper examines how France's Operation Barkhane contributed to political and security instability in Mali. It argues that despite early tactical success, the operation ultimately undermined state legitimacy, fueled anti-French sentiment, and created conditions that allowed jihadist groups to expand their influence. Through this lens, the study examines France's role in shaping regional power dynamics and the broader implications of foreign intervention in post-colonial states.

---

[248] Musée-Mémorial du terrorisme, *Defining Terrorism*, 2025.

[249] European Parliament, *Jihadist Terrorism in the EU Since 2015: Topics*, accessed July 22, 2025, https://www.europarl.europa.eu.

[250] Gabrielle Tejeda, "JNIM Expanding Geographic Reach and Staging Coordinated Attacks in the Sahel," *The Soufan Center*, June 5, 2025, https://thesoufancenter.org.

The research employs a qualitative case study approach, focusing specifically on Operation Barkhane and its effects on the northern part of Mali and the broader Sahel. It will explore the power dynamics between France and its former colonies during a counterterrorism operation. Operation Barkhane was chosen because it demonstrates the most direct actions the French took within the Sahel region. Data was collected through government documents, academic literature, and global databases, allowing for a comprehensive analysis of France's counterterrorism strategy and its long-term impact on regional stability.

The Republic of Mali

The Republic of Mali is located on a strip between the Sahara and the Sahel. During the 19th century, Mali was subjugated as a French colony.[251] Mali was known for being very rich in resources such as gold and other rare earth minerals, making it an enticing target. The French dug in and built forts, wanting to claim the region. By the late 19th century, the French had control of Mali along with a large part of the Sahara and Sahel. The French took full advantage of their colonies in Africa. During the First and Second World Wars, Mali and other parts of French-controlled Africa played a part in providing soldiers for the war effort.[252] Despite being a good source of soldiers for the World Wars, countries like Mali were often seen as less economically and politically important compared to others, such as Senegal and Côte d'Ivoire, and were treated as such, with forced labor and conscription being very common occurrences.[253]

In 1960, Mali gained full independence from France, following a brief period of autonomy beginning in 1958 under the French Community.[254]

---

[251] Agwuna Uzonna, "African Countries Colonized by France and Their Dates of Independence," *TalkAfricana*, 2023, https://www.talkafricana.com.

[252] James H. Morrow, "Black Africans in World War II: The Soldiers' Stories," *The Annals of the American Academy of Political and Social Science* 632 (2010): 12–25, https://doi.org/10.1177/0002716210361611.

[253] Encyclopædia Britannica, *History of Mali*, last modified 2025, https://www.britannica.com.

[254] *Mali*, *Oxford Reference*, 1997, https://www.oxfordreference.com.

This transition allowed Mali to establish its own government and political institutions. That same year, Mali and Senegal formed the Mali Federation, a short-lived union aimed at unifying newly independent former French colonies. However, the federation dissolved after Senegal withdrew, leading to the formal establishment of the Republic of Mali in 1960.[255] President Modibo Keïta subsequently distanced the country from France and aligned more closely with the Soviet Bloc — a move that contributed to political unrest and ultimately a military coup in 1968. Moussa Traoré, who seized power through the coup, was formally elected president in 1979. While he maintained diplomatic relations with both the Soviet Union and France — a strategy that found favor among segments of the population — his resistance to democratic reforms eventually led to his ousting in 1991.[256]

The coup and subsequent regional conflicts contributed to prolonged political instability in Mali, creating conditions that enabled the rise of extremist groups. This was marked by an increase in rebel activity and the growing presence of terrorist organizations, including jihadist networks and the Tuareg insurgency.[257] Despite losing formal control over its African colonies, including Mali, France maintained strong political, economic, and military ties with many of them — a policy framework often referred to as *Françafrique*. These post-colonial relationships persisted well into the 1990s, shaping diplomatic and security dynamics across the region.[258]

In the early 2010s, French President Emmanuel Macron maintained a cooperative relationship with Mali's then-president, Ibrahim Boubacar Keïta. This diplomatic rapport likely contributed to Keïta's decision to request French military assistance as domestic instability and insurgent violence escalated.[259]

---

[255] Dullah Omar Institute, *Mali*, August 15, 2023, https://www.dullahomarinstitute.org.

[256] *Encyclopædia Britannica*, *History of Mali*.

[257] *Tuareg Rebellion in Mali 1990–1995*, *Climate Diplomacy*, 2014, https://climate-diplomacy.org/case-studies/tuareg-rebellion-mali-1990-1995.

[258] Christophe Châtelot and Claude Bensimon, "How West African Public Opinion Turned Against France," *Le Monde*, November 3, 2023, https://www.lemonde.fr.

[259] Ministère de l'Europe et des Affaires étrangères. (n.d.). France and Mali. *France Diplomacy — Ministry for Europe and Foreign Affairs*. Retrieved from https://www.diplomatie.gouv.fr.

Operation Serval

In 2017, President Emmanuel Macron declared the Sahel a region of critical importance — not just for France, but for the European Union at large.[260] This framing set the tone for his administration's broader foreign policy in Africa, rooted in security, migration, and postcolonial influence. In 2012, Islamist militants began destabilizing the Sahel region, with Mali at the epicenter of the crisis. Facing widespread insecurity and ranked 176th on the Human Development Index (HDI), Mali lacked the capacity to address the threat independently and required external assistance.[261] In response, the Malian government called upon the West and the international community. In response to the escalating insurgency in northern Mali, France launched Operation Serval in January 2013, deploying approximately 5,000 troops — including Special Forces — to support the Malian government.[262] The operation aimed to drive out Islamist militants linked to groups such as AQIM and Ansar Dine, as part of a broader counterterrorism and counterinsurgency campaign. While the Tuareg rebellion initially contributed to the instability, Operation Serval was primarily focused on neutralizing jihadist threats rather than addressing the Tuareg separatist movement directly. As the precursor to Operation Barkhane, Operation Serval began at the request of the Malian government, which sought French military assistance to combat Islamist militants operating in the north. After stabilizing key areas and pushing back insurgent groups, France expanded its regional counterterrorism efforts, officially transitioning to Operation Barkhane in 2014. While the Tuareg rebellion contributed to the initial unrest, it was primarily a separatist movement rather than a jihadist threat. At the time, Tuareg nomads made up approximately five

---

[260] Máté Tánczos and Gergely Fejérdy, "Forced Withdrawal: The Case of France in the Sahel Region," *Journal of Central and Eastern European African Studies*, accessed July 22, 2025, https://jceeas.bdi.uni-obuda.hu/index.php/jceeas/article/view/242.

[261] Stéphane Spet, "Analyzing the French Strategy Against Jihadists in Mali," *Air & Space Power Journal — French Edition*, 2015, https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/volume-06_Issue-3/spet_e.pdf.

[262] Global Affairs, University of Navarra, "The Presence of the French Military in the Sahel: A Lasting Commitment or a Distant Fantasy?" accessed July 22, 2025, https://www.unav.edu/web/global-affairs/the-presence-of-the-french-military-in-the-sahel-lasting-commitment-or-distant-fantasy.

percent of Mali's population.[263] The purpose of Operation Serval was "to stop the jihadist advance; protect European and French nationals present in Mali; and restore Mali's territorial integrity"[264]. It was a direct military intervention in the region. Operation Serval was seen as a success, with enemy forces being pushed back. With Operation Serval largely viewed as a tactical success, France began to expand and adapt its counterterrorism strategy across the broader Sahel region.

Operation Barkhane

Operation Barkhane, launched in 2014, marked France's expanded military engagement in the Sahel, shifting from a national intervention in Mali to a regional counterterrorism campaign.[265] According to the French Ministry of Armed Forces, Barkhane's objective was "to fight armed terrorist groups in support of the armed forces of the G5 Sahel members and international forces, and to support local populations."[266] French forces operated across Burkina Faso, Chad, Mauritania, Mali, and Niger, though the majority remained concentrated in Mali.[267] Unlike Operation Serval, which had a narrow geographic and tactical focus, Barkhane aimed to stabilize the broader Sahel through sustained military presence and cross-border operations.[268]

---

[263] Dorina A. Bekoe, "Niger's Tuareg Rebellions," in *Niger: Will There Be a Third Tuareg Rebellion?* (Alexandria, VA: Institute for Defense Analyses, 2012), 2–5, http://www.jstor.org/stable/resrep26951.5.

[264] Virginie Baudais, Anouar Bourhrous, and Dylan O'Driscoll, "The Peacekeeping, Peacebuilding, and Security Architecture in the Sahel," in *Conflict Mediation and Peacebuilding in the Sahel: The Role of Maghreb Countries in an African Framework* (Stockholm: Stockholm International Peace Research Institute, 2021), 20–29, http://www.jstor.org/stable/resrep28281.10.

[265] France ONU, "France's Action in the Sahel," accessed July 22, 2025, https://www.franceonu.org.

[266] Virginie Baudais, Anouar Bourhrous, and Dylan O'Driscoll, "The Peacekeeping, Peacebuilding, and Security Architecture in the Sahel," in *Conflict Mediation and Peacebuilding in the Sahel: The Role of Maghreb Countries in an African Framework* (Stockholm: Stockholm International Peace Research Institute, 2021), 20–29, http://www.jstor.org/stable/resrep28281.10.

[267] Giovanni Faleg and Camilla Palleschi, "EU Member States' Power," in *African Strategies: European and Global Approaches Towards Sub-Saharan Africa* (Paris: European Union Institute for Security Studies, 2020), 34–44, http://www.jstor.org/stable/resrep26052.7.

[268] Stéphane Spet, "Analyzing the French Strategy Against Jihadists in Mali," *Air & Space Power Journal — French Edition*, 2015, https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/volume-06_Issue-3/spet_e.pdf.

The beginning of Operation Barkhane was seen as a tremendous success.[269] Within weeks, the French special forces captured towns back from the Jihadist rebels. Mali's initial response to France's swift military success was one of public gratitude and governmental approval, with many viewing the intervention as both timely and effective.[270] Operation Barkhane not only deployed troops to defend against the terror threat but also dispatched policemen and peacekeepers. Their role was to maintain order and assist on the civil side to prevent any local conflicts.[271]

Despite France's intention to neutralize terrorist threats in the Sahel, the security situation has continued to deteriorate, with violence spreading and militant groups gaining ground. n 2012, prior to Operation Serval, Mali ranked 22nd on the Global Terrorism Index; by 2025, it had risen to 4th, accounting for approximately 8 percent of global terrorism-related deaths.[272] As of 2024, Mali and the neighboring Sahelian states face escalating instability driven by the proliferation of extremist groups and fragmented military rule. This instability has caused multiple military coups and increased the presence of terror in the region.[273]

Consequences of Operation Barkhane

France's perceived overreach not only strained relations with local populations, but also alienated national governments. Over time, the countries that would go on to form the Alliance of Sahel States (AES) began expelling French forces from their territories and asserting greater control over their own security and governance. As Olech highlights:

---

[269] Isobel King, "How France Failed Mali: The End of Operation Barkhane," *Harvard International Review*, January 15, 2024, https://hir.harvard.edu/how-france-failed-mali-the-end-of-operation-barkhane.

[270] Ibid.

[271] Petitis, *The Sahel Intervention as a Case Study of France's Security Policy in Sub-Saharan Africa* (Athens: Hellenic Foundation for European and Foreign Policy, 2024), https://www.eliamep.gr/wp-content/uploads/2024/03/Policy-paper-157-.pdf.

[272] *Global terrorism index* (2025, March 5). Vision of Humanity. Retrieved from https://www.visionofhumanity.org.

[273] Pimentel, C. (2024, August 25). Mali's economic crisis: The instability following two political coups. *The Organization for World Peace*. Retrieved from https://www.worldpeace.org.

In the end of 2022, the presence of the French military forces was banned in Burkina Faso and this country followed Mali's hard path. Moreover, both states agreed to host the Wagner Group (Russian Mercenaries — private military company) that clearly showed the strong relation between two Sahel countries and Russia. At that point, France was not able to carry out its military operation against jihadists, being unable to fully operate on the territory of the G5 countries.[274]

The withdrawal of French forces from the Sahel has created a power vacuum that external actors, particularly Russia, have been quick to exploit. In the absence of French influence, several Sahel states have strengthened political and military ties with Russia. Some former French economic and security partnerships have since been replaced by Russian-backed initiatives and business interests.[275]

Following the removal of the French and other Western powers from the Sahel, Niger, Burkina Faso, and Mali formed a new regional bloc known as the Alliance of Sahel States (AES), with Burkina Faso taking a leadership role.[276] The alliance was designed as both a collective security pact and a political response to the perceived failure of external interventions. Shortly after its formation, all three countries formally withdrew from the Economic Community of West African States (ECOWAS), signaling a decisive break from Western-backed regional structures.[277]

Although established in late 2023, the AES has already drawn interest from other African states. According to recent reports, Côte d'Ivoire, Chad, Ghana, and Senegal have expressed varying degrees of support for

---

[274] Olech A. (2023) French Operation Barkhane in Africa — success or failure? (https://doi.org/10.12688/stomiedintrelat.17737.1).

[275] Banane, J.-P., Ford, Y., & Karr, L. (2025, April 3). Africa file, April 3, 2025: Russia-Sahel summit; Sahelian juntas target Chinese mining; M23 loses Walikale but Uganda leaves vacuum in North Kivu. *Institute for the Study of War*. Retrieved from https://www.understandingwar.org/backgrounder/africa-file-april-3-2025-russia-sahel-summit-sahelian-juntas-target-chinese-mining-.

[276] Ibid.

[277] Abdelhak Bassou et al., "From the Alliance of Sahel States to the Confederation of Sahel States: The Road Is Clear, but Full of Traps," *Policy Center for the New South*, April 24, 2024, https://www.policycenter.ma/publications/alliance-sahel-states-confederation-sahel-states-road-clear-full-traps.

the alliance and its security agenda.[278] To bolster its capacity, the AES has engaged Russia's Africa Corps to provide military support within member states, and it has begun acquiring Russian arms and logistical assistance.[279] This growing partnership has further expanded Russia's influence in the region, positioning Moscow as a strategic alternative to Western powers — a narrative reinforced by Russia's lack of colonial history in Africa.

Implications

The implications of the French having been removed from the Sahel go far beyond just France and their interest in the region. This has directly created a catalyst and example for other former colonies to band together and sever all ties with former colonial powers. This furthermore has allowed countries such as Russia and China to sink further into the Sahel and give them access to the local resources in the area[280].

Potentially, former colonizers such as France are still seen with a sense of omnipotence and omnipresence, as great powers, they could solve anything for those they once colonized. As they were in direct control of their countries for so long, they could be seen at the ultimate choice to remove a problem. French action in the Sahel directly disproved this notion and, rather than demonstrating competence, has allowed for a crack in the Western military façade and shown that their former colonizers are far from undefeatable. This shift may encourage the AES to consolidate power and assert greater regional autonomy, reducing its reliance on Western influence. This could result in a direct disruption of Western interests within the Sahel and set a precedent in Northern and Central Africa for

---

[278] Jean-Paul Banane, Yasmine Ford, and Liam Karr, "Africa File, April 3, 2025: Russia-Sahel Summit; Sahelian Juntas Target Chinese Mining; M23 Loses Walikale but Uganda Leaves Vacuum in North Kivu," *Institute for the Study of War*, April 3, 2025, https://www.understandingwar.org/backgrounder/africa-file-april-3-2025-russia-sahel-summit-sahelian-juntas-target-chinese-mining-.

[279] Rida Lyammouri, "For Mali and the Sahel, New Tensions and an Old—and Worsening—Security Problem," *Middle East Institute*, November 2021, https://www.policycenter.ma/publications/mali-and-sahel-new-tensions-and-old-%E2%80%94-and-worsening-%E2%80%94-security-problem.

[280] Szymon Czub, "The Decay of the Security Structure in the Sahel?" *Casimir Pulaski Foundation*, June 14, 2023, https://www.pulaski.pl.

attempting to address issues more in-house rather than relying on foreign powers. This may cause a more united Africa, with the AES now setting the example and other countries joining the alliance or creating their own coalition of nations to support Africa and African interests.

Conclusion

In conclusion, the French action within the Sahel has left a large power vacuum within the region. This is now being filled by both local governments and new organizations such as the AES or other groups such as Boko Haram, ISIS, JMIN, and the African Corps.

Seen in a more optimistic light, this power vacuum could create an opportunity for greater African unity, emphasizing regional cooperation over dependence on Western partners. The SAE is an example of this, with the Sahel coming together to form an alliance while staying in-house, rather than relying on Western powers. This void does, however, open the potential for exploitation by other organizations. While the West may no longer be fully accepted within the Sahel, this does not mean its replacement will be better or any more of a force for good in the region. However, this topic is very complex, and more research is needed to further assess the security-related implications, such as how other countries are reacting to this situation. Potentially, it would be prudent to examine other countries in the region affected primarily by eastern powers, such as Russia and China, and determine how, if at all, Operation Barkhane has influenced the opinions of other countries regarding Western powers in Africa and the West's role on the continent.

Bibliography

Banane, Jean-Paul, Yasmine Ford, and Liam Karr. *Africa File, April 3, 2025: Russia-Sahel Summit; Sahelian Juntas Target Chinese Mining; M23 Loses Walikale but Uganda Leaves Vacuum in North Kivu*. Institute for the Study of War, April 3, 2025. https://www.understandingwar.org/backgrounder/

africa-file-april-3-2025-russia-sahel-summit-sahelian-juntas-target-chinese-mining.

Bassou, Abdelhak, et al. *From the Alliance of Sahel States to the Confederation of Sahel States: The Road Is Clear, but Full of Traps*. Policy Center for the New South, April 24, 2024. https://www.policycenter.ma/publications/alliance-sahel-states-confederation-sahel-states-road-clear-full-traps.

Baudais, Virginie, Anouar Bourhrous, and Dylan O'Driscoll. "The Peacekeeping, Peacebuilding and Security Architecture in the Sahel." In *Conflict Mediation and Peacebuilding in the Sahel: The Role of Maghreb Countries in an African Framework*, 20–29. Stockholm: Stockholm International Peace Research Institute, 2021. http://www.jstor.org/stable/resrep28281.10.

Bekoe, Dorina A. "Niger's Tuareg Rebellions." In *Niger: Will There Be a Third Tuareg Rebellion?*, 2–5. Alexandria, VA: Institute for Defense Analyses, 2012. http://www.jstor.org/stable/resrep26951.5.

Berger, Cécile. *What Role for NATO in the Sahel?* NATO Defense College, 2021. http://www.jstor.org/stable/resrep39560.

Châtelot, Christophe, and Claude Bensimon. "How West African Public Opinion Turned Against France." *Le Monde*, November 3, 2023. https://www.lemonde.fr/en/le-monde-africa/article/2023/11/03/how-west-african-public-opinion-turned-against-france_6223881_124.html.

Climate Diplomacy. "Tuareg Rebellion in Mali 1990–1995." 2014. https://climate-diplomacy.org/case-studies/tuareg-rebellion-mali-1990-1995.

Council on Foreign Relations. "Violent Extremism in the Sahel." *Global Conflict Tracker*. Accessed July 22, 2025. https://www.cfr.org/global-conflict-tracker/conflict/violent-extremism-sahel.

Czub, Szymon. "The Decay of the Security Structure in the Sahel?" *Casimir Pulaski Foundation*, June 14, 2023. https://pulaski.pl/en/the-decay-of-the-security-structure-in-the-sahel.

Dullah Omar Institute. "Mali." August 15, 2023. https://dullahomarinstitute.org.za/acjr/resource-centre/mali.

Encyclopædia Britannica. "History of Mali." *Encyclopædia Britannica*. Accessed July 22, 2025. https://www.britannica.com/topic/history-of-Mali.

European Parliament. "Jihadist Terrorism in the EU Since 2015: Topics." Accessed July 22, 2025. https://www.europarl.europa.eu/topics/en/article/20180703STO07127/jihadist-terrorism-in-the-eu-since-2015.

Faleg, Giovanni, and Camilla Palleschi. "EU Member States' Power." In *African Strategies: European and Global Approaches Towards Sub-Saharan Africa*,

34–44. Paris: European Union Institute for Security Studies, 2020. http://www.jstor.org/stable/resrep26052.7.

France ONU. "France's Action in the Sahel." Accessed July 22, 2025. https://onu.delegfrance.org/france-s-action-in-the-sahel.

King, Isobel. "How France Failed Mali: The End of Operation Barkhane." *Harvard International Review*, January 15, 2024. https://hir.harvard.edu/how-france-failed-mali-the-end-of-operation-barkhane.

Lyammouri, Rida. "For Mali and the Sahel, New Tensions and an Old — and Worsening — Security Problem." *Middle East Institute*, November 2021. https://www.policycenter.ma/publications/mali-and-sahel-new-tensions-and-old-%E2%80%94-and-worsening-%E2%80%94-security-problem.

Ministère de l'Europe et des Affaires étrangères. "France and Mali." *France Diplomacy – Ministry for Europe and Foreign Affairs*. Accessed July 22, 2025. https://www.diplomatie.gouv.fr/en/country-files/mali/france-and-mali-65154.

Morrow, James H. "Black Africans in World War II: The Soldiers' Stories." *The Annals of the American Academy of Political and Social Science* 632 (2010): 12–25. http://www.jstor.org/stable/27895945.

Musée-Mémorial du Terrorisme. "Defining Terrorism." Accessed July 22, 2025. https://musee-memorial-terrorisme.fr/en/defining-terrorism.

Nuzki, Clara. "The New Alliance of Sahel States and the Future of Africa's Legacy Institutions." *The Youth Bloom | CSIS Podcasts*. 2025. https://www.csis.org/podcasts/youth-bloom/new-alliance-sahel-states-and-future-africas-legacy-institutions.

Olech, Anna. "French Operation Barkhane in Africa — Success or Failure?" *Stosunki Międzynarodowe — International Relations* 3, no. 17 (2023). https://doi.org/10.12688/stomiedintrelat.17737.1.

Oxford Reference. "Mali." 1997. https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100128742.

Petitis. *The Sahel Intervention as a Case Study of France's Security Policy in Sub-Saharan Africa*. Athens: Hellenic Foundation for European and Foreign Policy, 2024. https://www.eliamep.gr/wp-content/uploads/2024/03/Policy-paper-157-.pdf.

Pimentel, Cristina. "Mali's Economic Crisis: The Instability Following Two Political Coups." *The Organization for World Peace*, August 25, 2024. https://theowp.org/malis-economic-crisis-the-instability-following-two-political-coups.

Spet, Stéphane. "Analyzing the French Strategy Against Jihadists in Mali." *Air & Space Power Journal — French Edition*, 2015. https://www.airuniversity.af.edu/Portals/10/ASPJ_French/journals_E/volume-06_Issue-3/spet_e.pdf.

Tánczos, Máté, and Gergely Fejérdy. "Forced Withdrawal: The Case of France in the Sahel Region." *Journal of Central and Eastern European African Studies*.

Accessed July 22, 2025. https://jceeas.bdi.uni-obuda.hu/index.php/jceeas/article/view/242.

Tejeda, Gabrielle. "JNIM Expanding Geographic Reach and Staging Coordinated Attacks in the Sahel." *The Soufan Center*, June 5, 2025. https://thesoufancenter.org/intelbrief-2025-june-5.

University of Navarra — Global Affairs. "The Presence of the French Military in the Sahel: A Lasting Commitment or a Distant Fantasy?" Accessed July 22, 2025. https://www.unav.edu/web/global-affairs/the-presence-of-the-french-military-in-the-sahel-lasting-commitment-or-distant-fantasy.

Vision of Humanity. *Global Terrorism Index 2025 — World*. March 5, 2025. https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf.

4

Beyond PREVENT: Reimagining Predictive Policing through Ethical Algorithms and Behavioral Insight

Medha KALIDAS

Abstract: The UK's PREVENT strategy, originally designed to prevent radicalization through early intervention, has been facing increasing criticism for enabling racial bias and generating an overwhelming number of false referrals. This paper critically evaluates the program's reliance on human-led referrals and draws attention to confirmation bias and the resulting distrust within minority communities. The paper then examines the potential of predictive policing tools like Geolitica (formerly PredPol) to reduce human error, while also acknowledging that bias is replicated when manmade data is input. Building on these critiques, but aiming to keep the idea of predictive algorithms intact, I propose an ethically guided reform to predictive algorithms that is centered on behavior-based indicators, community involvement, and transparency. Finally, I acknowledge the presence of AI and its relevance in our current world. I explore potential avenues of future research with this information, all with the goal of legitimizing future counterterrorism initiatives.

Keywords: Algorithmic Bias, Confirmation Bias, Predictive Policing, Counter-radicalization, Ethical AI, UK PREVENT, Geolitica (PredPol)

Introduction

In 2015, Mohammed Umar Farooq, a Global Security student at Staffordshire University, was reading a textbook titled Terrorism Studies when he was falsely accused of being a terrorist by a campus official.[281] Farooq, interrogated under the premise of the anti-extremism initiative UK PREVENT, has become one of many minorities suspected of terrorism since the creation of the initiative.[282] Introduced in 2003 as part of the UK's broader CONTEST counter-terrorism initiatives, PREVENT was designed to stop individuals from becoming terrorists by intervening before a crime could possibly occur.[283] It relies on public sector workers, from teachers to healthcare professionals, to report individuals they suspect of radicalization to the local police. By 2015, this duty became a legal mandate across institutions within the UK, with Staffordshire University being one of many schools to adopt the protocol. However, in practice, false accusations (like Farooq's case) negatively impact the UK PREVENT's legacy.

Recent data, disclosed by the National Police Chiefs' Council, following a freedom of information request by Rights & Security International, highlights just how widespread the impact of false accusations spreads when purely reliant on human referral.[284] In 2024 alone, 6,922 individuals were referred to as PREVENT. Yet, only 512 of these (7%) were adopted as Channel cases, meaning that more than 90% of referrals were either misclassified or did not meet the threshold for concern.[285] Channel cases are

---

[281] Randeep Ramesh and Josh Halliday, "Student Accused of Being a Terrorist for Reading Book on Terrorism," *The Guardian*, September 24, 2015, https://www.theguardian.com/education/2015/sep/24/student-accused-being-terrorist-reading-book-terrorism.

[282] Paul Dresser, Mike Rowe, and Jamie Harding, "Unintended Consequences of Public-Facing Counter-Terrorism Training and Vigilance Campaigns on Minority Groups," *Critical Studies on Terrorism*, March 27, 2025: 1–28, https://doi.org/10.1080/17539153.2025.2479912.

[283] Counter Terrorism Policing, "Prevent," *UK Counter Terrorism Policing*, accessed July 16, 2025, https://www.counterterrorism.police.uk/what-we-do/prevent.

[284] Home Office, "Individuals Referred to and Supported Through the Prevent Programme, April 2023 to March 2024," *GOV.UK*, accessed July 16, 2025, https://www.gov.uk/government/statistics/individuals-referred-to-prevent-to-march-2024/individuals-referred-to-and-supported-through-the-prevent-programme-april-2023-to-march-2024.

[285] Rights & Security International, "Written Evidence (GIS0017) to the Women and Equalities Committee," *UK Parliament Committees*, 2023, https://committees.parliament.uk/writtenevidence/139769/pdf.

those referrals to the UK PREVENT program that, after initial reporting, are reviewed by a multi-agency panel (including police, health, education and social services) using the Channel Vulnerability Assessment Framework. Individuals deemed "vulnerable to being drawn into terrorism" receive structured support — such as tailored mentoring, mental-health interventions and community-based assistance — to address risk factors before any offence occurs.[286] Despite PREVENT's stated goal of "identifying ideological extremism", the single largest referral category (36%) involved individuals with "vulnerability present but no ideology or counterterrorism risk." 23% of adopted Channel cases in 2024 were still focused on suspected Islamist radicalization, despite years of documented decline.[287] PREVENT, in its current state, is ineffective, so the question and challenge then is, how can we improve the referral process to reduce false accusations and streamline the job of law enforcement?

PREVENT's current human-led referral system reinforces racial bias and has been shown to fail its stated goals regarding counter-radicalization. Based on these issues, I propose a roadmap of ethically centered solutions using predictive models that would significantly reduce the human error and biases found in a referral-led system. Looking ahead, I consider how AI is likely to integrate into global counterterrorism efforts as part of this evolving landscape.

This paper proceeds in five sections. The first section critically examines PREVENT as a case study, highlighting issues in a referral-based counter-radicalization program, highlighting its main issue of distinguishing legitimate threats from racialized assumptions. In the second section, explores a possible predictive policing model based on Geolitica (formerly PredPol).[288] Then in section three, it acknowledges shortcomings of Geolitica in reports of algorithmic bias through local opinions. Section four offers a detailed proposal for integrating more advanced systems and AI into a reimagined PREVENT model, which features behavior-based input,

---

[286] Ibid.

[287] Rights & Security International, *"Written Evidence,"* 2023.

[288] Geolitica, "Company Overview," *Geolitica*, accessed July 3 2025, https://geolitica.com/company.

transparency regarding "referrals," and increased incorporation of community feedback. Finally, in section five, it zooms out and addresses larger critiques and the real-world impact of normalizing AI into predictive policing/ counter-radicalization programs, and takes a look at a future where AI is sure to stay.

A Critique on UK Prevent: Prevailing Issues with Human Bias

The UK's PREVENT strategy, while initially conceived in 2003 as a proactive tool to prevent vulnerable individuals from extremism, has now transformed into a program that encourages the targeting of Muslim and minority communities under the guise of prevention.[289] Studies have shown that the strategy operates through racialized assumptions about risk, with early implementations specifically targeting areas with 2% or higher Muslim demographics, and has resulted in the systematic marginalization of Muslim minorities through discriminatory referral practices.[290] The program inherently relies on the referrals of local community members, like teachers, doctors, nurses, and police officers, to spot potential radicals and report them to the program. PREVENT has enabled a system where its effectiveness hinges purely on human judgment.[291] These judgments, caused by implicit cognitive biases like confirmation bias, only reinforce the idea that basing a system on human judgment leads to biased results.[292]

A 2021 report by Amnesty International UK criticized PREVENT, noting how the program operates through a vague definition of extremism that leaves too much room for interpretation. This ambiguity, cultivated in

---

[289] Ibid.

[290] Lee Jarvis and Stuart Macdonald, "Disinformation in the UK's Prevent Strategy: Preventing Prevent?," *Crime, Media, Culture* 19, no. 2, 2023: 175–192, https://doi.org/10.1177/17461979221077990; Craig L. Hughes and John Lea, "PREVENT and the Ungovernable Other: Poststructuralism, Counter-Extremism, and the Securitisation of British Muslims," *Critical and Radical Social Work* 12, no. 4 (2024): 559–574, https://doi.org/10.1332/204986024X17128447216210.

[291] Ibid.

[292] Ibid.

communities experiencing increased Islamophobic sentiment and reinforced by a "statutory duty to report potential signs of radicalization," pressures these local community members to report, even when unnecessary. The result is what Amnesty International found and identifies as a pattern of "racialized referrals" (e.g., Mohammed Farooq, children flagged for discussing political issues/ expressing personal distress).[293]

Additional data has supported these concerns. From 2019 to 2024, the National Police Chiefs' Council disclosed that over 16,000 referrals were made, but there was a disproportionate percentage involving Asian, Black, and Middle Eastern individuals. For example, Black individuals constituted 7.9% of referrals but just 2.5% of the general population.[294] This data is only a fraction of the systemic profiling found within UK PREVENT.

Furthermore, scholars have linked this structural bias to the psychological process of confirmation bias.[295] Referrers of UK PREVENT are not immune to this logic. In terms of PREVENT, people may unconsciously seek behaviors that validate their assumptions about who is likely to radicalize- this is a prime example of confirmation bias.[296] Radicalization is a non-linear and deeply contextual process. Yet, PREVENT training modules are rooted in superficial checklists of behavioral signs, such as "withdrawal from peers" or "interest in foreign conflicts", which can mislabel normal actions as a precursor to terrorism.[297] Confirmation bias, guiding questions, and systemic flaws within PREVENT lead to a slew of issues.

These misjudgments highlight PREVENT's core issues. Referrals, even when not adopted as Channel cases, are still logged into police databases, stigmatize individuals and alienate them from their community, and enhance distrust of counter-radicalization practices and law enforcement. A report

---

[293] Ibid.

[294] Ibid.

[295] Risa Fahriyani Purnamawati, "The Role of Cognitive Bias in Principal Decision Making: A Narrative Analysis of the Literature," *PPSDP International Journal of Education* 3, no. 2, October 22, 2024, https://doi.org/10.59175/pijed.v3i2.310.

[296] Suresh Grover, *Racial Profiling and Counter-Terrorism in Britain: A Critical Race Perspective* (Malmö University, 2018), https://www.diva-portal.org/smash/get/diva2:1237959/FULLTEXT01.pdf.

[297] Grover, *Racial Profiling and Counter-Terrorism*, 2018.

from the Center for the Resolution of Intractable Conflict showcases that such practices make communities less likely to cooperate with future security efforts as well, which could cause future issues.[298]

In total, the PREVENT strategy's reliance on subjective judgment, led by humans who inherently have bias, has been shown to undermine its legitimacy as a counter-radicalization tool. In the next section, I will explore whether and how predictive algorithms, as a supplement, could offer more precise, fair, and transparent means of identifying potential threats.

Learning from Predictive Algorithms through Geolitica

Predictive policing refers to the use of algorithms and data analytics to anticipate and "predict" where crimes are likely to occur, or who might even be involved in them.[299] It has been adopted by several justice agencies to optimize law enforcement efforts and is increasingly debated in counterterrorism contexts. By identifying spatial or behavioral patterns associated with previous crimes, using a scoring system to rank individuals likely to participate in more crime, predictive policing, as we know it, aims to offer a more data-driven means of preempting threats. However, in recent years, backlash regarding algorithmic bias and the effectiveness of these programs has raised questions. Thus the question emerges, is it feasible to train and guide the development of the algorithms used for predictive policing to reduce human bias?

Let us first take a look at PredPol (now Geolitica).[300] Originally designed to predict the location and timing of crimes based on historical data, the model divides cities into small spatial grids and updates predictions throughout the day based on recent arrests, reported incidents, and police

---

[298] Ibid.

[299] "Predictive Policing," *EBSCO Research Starters: Social Sciences and Humanities*, accessed July 8, 2025, https://www.ebsco.com/research-starters/social-sciences-and-humanities/predictive-policing.

[300] Ibid.

activity. This "crime weather forecast" informed police patrol routes and resource allocation in more than sixty jurisdictions at its peak.[301] At first glance, Geolitica appears to address the core issue of a program like UK PREVENT that relies purely on subjective human referrals. By automating pattern recognition, current predictive policing tools claim to remove emotion, prejudice, and inconsistency from decision-making.

Despite this apparent objectivity, however, lies a deeper issue, where data is based on historical police activity. A biased input leads to a biased output. A computer/ system/ algorithm learns from existing arrest rates, call records, and incident reports. So, it can be taught bias by feeding it information already based on the errors of human judgment. Cities like Santa Cruz and Los Angeles, because of this, discontinued PredPol entirely.[302] A 2023 analysis found that the algorithm disproportionately flagged communities of color and offered little transparency about how it generated these predictions or how it was being audited.[303]

However, if the transparency of usage would be increased, predictive algorithms could outperform human judgment.[304] The challenge lies not in technical capacity but ethical policy and structure, where transparency to people and accountability by law enforcement are prioritized.[305] The failures of Geolitica showcase a blueprint for predictive policing reform that could not only be used in local law enforcement but also extend to counter radicalization programs like PREVENT.

---

[301] Will Douglas Heaven, "Predictive Policing Algorithms Are Starting to Fail," *MIT Technology Review*, February 13, 2020, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice.

[302] Ibid.

[303] Yale Law School Media Freedom & Information Access Clinic, *Geolitica: Predictive Policing and Racial Bias*, 2023, https://law.yale.edu/sites/default/files/area/center/mfia/document/infopack.pdf.

[304] Ibid.

[305] Europol Innovation Lab, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement* (Luxembourg: Publications Office of the European Union, 2024), https://www.europol.europa.eu.

An Ethically Guided Proposal for Predictive Policing and Preventative Measures

Learning from the failures and inherent biases in PredPol, we can look at possible methods of improving algorithms.[306] We should move from identity-based data to behavioral indicators. Stripping predictive models of identity-based data like race and zip code and moving to the development of algorithms based on behavioral indicators would significantly reduce the amount of bias input within the system. By removing racial and socioeconomic data from predictive models, we stop continuing the aftereffects of over policing. In practice, the replacement of this data could be to use verified indicators of radicalism.[307] These include, but are not limited to: consistent engagement with extremist websites, chat rooms, and forums, documented attempts to procure weapons and consistent travel to regions prone to threat. Using data from the Royal United Services Institute (RUSI) for Defence and Security Studies, we can train machine learning models only on this information, and supplement this to counter-radicalization programs.[308] By changing the input variables into the algorithms we use, we significantly decrease the likelihood of biased output.

n addition, several Los Angeles locals outlined to police using PredPol that the community should be more involved in preemptive policing practices, after several people were wrongfully accused.[309] Using heavy community oversight would increase accountability within law enforcement.[310] I propose a locally elected community board that has the power to suggest and veto pilot predictive models used in their own city. In practice, this would ensure that each jurisdiction using predictive tools would be required to

---

[306] Royal United Services Institute (RUSI), *Algorithms and Bias in Policing: Examining Evidence, Debates and Calls for Reform*, *RUSI*, accessed July 16, 2025, https://www.rusi.org/explore-our-research/publications/briefing-papers/data-analytics-and-algorithmic-bias-policing.

[307] Ibid.

[308] Ibid.

[309] Sarah Brayne, "Big Data Surveillance: The Case of Policing," *American Sociological Review* 82, no. 5, October 2017: 977–1008, https://doi.org/10.1177/0003122417725865.

[310] Beth Pearsall, "Predictive Policing: The Future of Law Enforcement?" *NIJ Journal*, no. 266, 2010: 16–19, https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement.

submit quarterly reports on system outputs and false positives, include an appeals process for those accused of radicalism, and include a community board for pilot initiatives. According to RUSI, external scrutiny by the community is needed for these systems to not only be technically proficient, but also ethically.[311]

These are only two possible methods that could significantly improve predictive models. Looking towards the future, it is not practical to entirely abandon technology, but to rethink its functions and increase accountability. We must also acknowledge the topic of AI in this argument and its implications within the world of counter-radicalization.

A Future of AI and Counter-Radicalization

As predictive policing will evolve, artificial intelligence is no longer a hypothetical. From deep neural networks capable of behavior prediction to AI-based surveillance tools, the future of counter-radicalization will be algorithmically shaped.[312]

Research on future AI-based counter-radicalization initiatives will require understanding topics of standardized data-sharing protocols, a more concrete and universal definition of extremism, and increased international cooperation regarding the ethics of AI.[313] These topics all raise vital questions. How can democratic states prevent AI misuse if they are working/cooperating with authoritarian regimes? What does accountability look like in preventing intelligence sharing from becoming a vehicle of repression, like Pegasus spyware, or INTERPOL red notices?[314]

---

[311] Ibid.

[312] Waddah Wael Saeed and Christian Omlin, "An Overview of AI Applications in Policing and Public Safety," *Knowledge-Based Systems* 258 (2023), https://doi.org/10.1016/j.knosys.2023.110715.

[313] George Mohler et al., "A Penalized Likelihood Method for Balancing Accuracy and Fairness in Predictive Policing," *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2018: 2454–2459, https://doi.org/10.1109/SMC.2018.00421.

[314] Philip M. Napoli, "Social Media and the Public Interest: Governance of News Platforms in the Realm of Algorithmic Accountability," *University of Pennsylvania Law Review* 168, no. 6, 2020: 1381–1432, https://scholarship.law.upenn.edu/penn_law_review/vol168/iss6/4.

These two questions are some of many that are deeply underexplored, but are crucial for us to understand what role AI will play in the future of counterterrorism.

Conclusion

UK PREVENT began with the ambition of preventative measures. However, as demonstrated in this article, its current reliance on human-led referrals has resulted in a general failure of the system, stemming from confirmation bias and racialized assumptions. Over 90% of referrals result in no further action, but the impact false accusations have on individuals is lasting.

The first section displayed how PREVENT's subjective nature encourages over-reporting, especially against Muslim and minority populations, and how vague indications of "extremism" turn normal behavior into grounds for suspicion. Building on this, the second section looked at a possible algorithmic solution to predictive policing, using PredPol as a case study. However, this also revealed that when trained on biased datasets and with no accountability regarding usage, predictive models simply replicate the problems of human bias. So, considering this information, but choosing not to scrap the idea of predictive tools entirely, the third section offered a proposal. With behavioral rather than identity and socioeconomic-based indicators, audits, or community involvement, predictive models could serve as more equitable components to traditional counter-radicalization strategies. Finally, the fourth section highlighted the current and growing role of AI in counter-radicalization. The core question moving forward is not if AI will influence counterterrorism, but rather how democratic societies can ethically regulate and apply these tools. Future research must therefore prioritize defining clear international standards for AI governance and accountability especially urgent given the rapid deployment of AI by authoritarian regimes. In doing so, predictive technologies can be leveraged not merely to identify threats, but to better understand radicalization itself, significantly reducing bias and improving the effectiveness of counterterrorism efforts overall.

Bibliography

Amnesty International. *'This Is the Thought Police': The Prevent Duty and Its Chilling Effect on Human Rights.* Amnesty International UK, 2023.

"Archived | Predictive Policing: The Future of Law Enforcement? | National Institute of Justice." Accessed July 8, 2025. https://nij.ojp.gov/topics/articles/predictive-policing-future-law-enforcement.

Brayne, Sarah. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82, no. 5 (October 2017): 977–1008. https://doi.org/10.1177/0003122417725865.

"Company." Accessed July 8, 2025. https://geolitica.com/company.

Counter Terrorism Policing. "Prevent." Accessed July 8, 2025. https://www.counterterrorism.police.uk/what-we-do/prevent.

"Data Analytics and Algorithmic Bias in Policing." Accessed July 8, 2025. https://www.rusi.org.

Dresser, Paul, Mike Rowe, and Jamie Harding. "Unintended Consequences of Public-Facing Counter-Terrorism Training and Vigilance Campaigns on Minority Groups." *Critical Studies on Terrorism* 18, no. 2 (April 3, 2025): 450–77. https://doi.org/10.1080/17539153.2025.2479912.

Europol. "AI and Policing — The Benefits and Challenges of Artificial Intelligence for Law Enforcement." Accessed July 8, 2025. https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing.

GOV.UK. "Individuals Referred to and Supported through the Prevent Programme, April 2023 to March 2024." Accessed July 8, 2025. https://www.gov.uk/government/statistics/individuals-referred-to-prevent-to-march-2024/individuals-referred-to-and-supported-through-the-prevent-programme-april-2023-to-march-2024.

Grover, Suresh. *Racial Profiling and Counter-Terrorism in Britain: A Critical Race Perspective.* Malmö University, 2018. https://www.diva-portal.org/smash/get/diva2:1237959/FULLTEXT01.pdf.

Hughes, Craig L., and John Lea. "PREVENT and the Ungovernable Other: Post-structuralism, Counter-Extremism, and the Securitisation of British Muslims." *Critical and Radical Social Work* 12, no. 4 (2024): 559–574. https://bristoluniversitypressdigital.com/view/journals/crsw/12/4/article-p559.xml.

"MIT Technology Review. "Predictive Policing Algorithms Are Racist. They Need to Be Dismantled." Accessed July 8, 2025. https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice.

Liden, Moa. *Confirmation Bias in Criminal Cases.* n.d. https://global.oup.com/academic/product/confirmation-bias-in-criminal-cases-9780192867643?cc=us&lang=en&.

Mohler, George, Rajeev Raje, Jeremy Carter, Matthew Valasik, and Jeffrey Brantingham. "A Penalized Likelihood Method for Balancing Accuracy and Fairness in Predictive Policing." In *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2454–59. 2018. https://doi.org/10.1109/SMC.2018.00421.

"Predictive Policing | EBSCO Research Starters." Accessed July 8, 2025. https://www.ebsco.com/research-starters/social-sciences-and-humanities/predictive-policing.

Ramesh, Randeep, and Josh Halliday. "Student Accused of Being a Terrorist for Reading Book on Terrorism." *The Guardian*, September 24, 2015, sec. Education. https://www.theguardian.com/education/2015/sep/24/student-accused-being-terrorist-reading-book-terrorism.

Saeed, Waddah, and Christian Omlin. "Explainable AI (XAI): A Systematic Meta-Survey of Current Challenges and Future Opportunities." *arXiv*, November 11, 2021. https://doi.org/10.48550/arXiv.2111.06420.

Yale Law School. "Algorithmic Accountability White Paper." Accessed July 8, 2025. https://law.yale.edu/mfia/projects/algorithmic-accountability/algorithmic-accountability-white-paper.

Zempi, Irene, and Athina Tripli. "Listening to Muslim Students' Voices on the Prevent Duty in British Universities: A Qualitative Study." *Education, Citizenship and Social Justice* 18, no. 2 (2022): 230–245. https://doi.org/10.1177/17461979221077990.

PART III

SECURITY AND TECHNOLOGY

1

Cyber Diplomacy in the Age of Artificial Intelligence: The Emerging Role of Diplomats and Embassies in a Data-Driven World

Irwin SALAZAR

Abstract: This paper explores how Artificial Intelligence is reshaping cyber diplomacy, particularly by transforming core diplomatic functions and management of embassies in digital environments. The study draws on Constructivism, Liberal institutionalism, and Institutional Adaptation Theory to assess how AI influences diplomatic practices and challenges existing structures of global governance. Through a comparative analysis of the EU, U.S., and China, the paper argues that effective AI-enabled diplomacy must balance technological innovation with ethical accountability to remain legitimate and functional in an increasingly fragmented international system.

Keywords: Cyber Diplomacy, Artificial Intelligence, Diplomats, Embassies, Digital Transformation

Introduction

Traditional diplomacy functions as the base of international relations through direct negotiations, ambassadorial roles and official government-to-government communication. The digital transformation of statecraft has brought forth fresh diplomatic approaches. *Digital*

diplomacy uses information and communication technologies (ICTs) to reach out to the public while *cyber diplomacy* focuses on creating rules and security frameworks for cyberspace. Artificial Intelligence (AI) intersects with all forms of diplomacy but it transforms cyber diplomacy most significantly because it shapes both diplomatic tools and diplomatic environments.

AI has emerged as a force multiplier in global affairs which requires new standards for diplomatic conduct and organization.[315] The transformation is most evident in cyber diplomacy through state negotiations about cyberspace governance[316], cybersecurity[317] and responsible state conduct. The implementation of AI technology brings both practical advantages and ethical challenges which reshape how diplomatic actors define themselves and perform their functions and organizational structure. The data-driven nature of modern society requires cyber diplomacy to address both emerging threats and changes in governance systems and epistemic authority and geopolitical competition. This paper seeks to investigate the impact of AI on cyber diplomacy development and implementation alongside diplomatic and embassy responses to these challenges and required institutional measures for effective international engagement.

---

[315] The European Commission defines Artificial Intelligence as software that uses machine learning and logic- and knowledge-based approaches to generate predictions, recommendations, or decisions which affect real or virtual environments for human-defined objectives. See European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM(2021) 206 final, (Brussels, 2021); OECD, *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2019).

[316] Cyberspace governance requires the creation of norms and principles alongside rules and procedures which direct state actions and institutional practices and technological advancements in digital space. The United Nations Group of Governmental Experts (GGE) published A/70/174 (2015) to report on information and telecommunications developments in international security while Joseph S. Nye Jr. wrote "The Regime Complex for Managing Global Cyber Activities" for the Global Commission on Internet Governance Paper Series no. 1 (2014).

[317] The International Telecommunication Union (ITU) defines cybersecurity as "the collection of tools, policies, security concepts, safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." This includes information security, network security, and the protection of infrastructure from unauthorized access or attacks. See International Telecommunication Union, ITU National Cybersecurity Strategy Guide, 2nd ed. (Geneva: ITU, 2018), 5, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx.

This paper addresses the following research questions:

1. Through what mechanisms does AI transform the field of cyber diplomacy?
2. In what ways does AI integration change the roles and responsibilities of diplomats and embassies?
3. What are the primary challenges and advantages that AI introduces into international diplomatic practice?

The central hypothesis of this research is that AI enhances the efficiency and effectiveness of cyber diplomacy by enabling advanced data analysis, communication, and decision-making. However, its adoption also necessitates a transformation in diplomat roles, requiring the development of technological competencies and adaptability. Consequently, embassies must implement AI-enabled strategies to remain relevant and effective with the evolving international system.

Conceptual Clarifications: Cyber Diplomacy and its Boundaries

The definition of cyber diplomacy needs clarification because it shows similarities with other related concepts such as digital diplomacy, e-diplomacy and virtual diplomacy. *Digital diplomacy* refers to the use of digital tools and platforms including social media and websites to improve traditional diplomatic functions such as public outreach and consular services. *E-diplomacy* has a similar meaning to digital diplomacy because it involves using internet technologies to enhance diplomatic communication and information management through secure email systems and internal coordination tools for foreign affairs ministries. *Virtual diplomacy* goes beyond digital platforms by allowing diplomatic relations through remote virtual environments which have become the new standard for multilateral negotiations and crisis communications since the COVID-19 pandemic.[318]

[318] Brian Hocking and Jan Melissen, *Diplomacy in the Digital Age* (The Hague: Clingendael Institute, 2015), 7–10; and Aytaj Allahverdiyeva, "Reframing the Pandemic-Era Digitalization of Diplomacy: From Virtual Representation to Virtual Diplomacy," *Place Branding and Public Diplomacy* (2023), https://doi.org/10.1057/s41254-023-00296-1.

Cyber diplomacy describes diplomatic efforts that focus on technology instead of using technology for diplomatic purposes. The negotiation process creates rules and norms and institutional arrangements which govern cyberspace through cybersecurity treaties and cybercrime conventions and multilateral protocols for digital environment state behavior. According to Barrinha and Renard cyber diplomacy functions as a normative framework which seeks to establish an "international society" within cyberspace despite its historical characteristics of fragmentation, asymmetry and normative disputes.[319]

The distinction holds special importance for studying Artificial Intelligence. AI operates as both a diplomatic instrument and a global governance entity while dissolving distinctions between these categories. AI functions as a digital diplomatic tool for strategic communication and engagement while creating new challenges regarding norm-setting and transparency and attribution and sovereignty in cyber diplomacy. The implementation of AI in diplomacy demands both clear conceptual definitions and awareness of established norms. The evaluation of AI's transformative impact on twenty-first-century statecraft depends on understanding how these forms interact with each other.

Literature Review

The academic discussion about cyber diplomacy has developed substantially because of its increasing importance in international relations and institutional practice. The initial definitions of cyber diplomacy concentrated mainly on diplomatic measures against cybersecurity threats. As Christou argues, cyber diplomacy combines conflict resolution in the cyber domain with broader efforts to build cooperation — particularly through tackling cybercrime and strengthening institutional capacity.[320] Attatfa et al. conducted a systematic review which

[319] André Barrinha and Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, no. 4–5 (2017): 353–364.

[320] George Christou, "Cyber Diplomacy: The Making of an International Society in the Digital Age," *Global Society* 30, no. 3 (2016): 321–337, https://doi.org/10.1080/13600826.2016.1158204.

showed that the term encompasses both state-led and multilateral initiatives for online behavior regulation and digital security governance structure development.[321]

Barrinha and Renard contend that cyber diplomacy serves as a tool to establish an international society in cyberspace which functions as a normative framework to promote order and rule-making and cooperative threat management.[322] This perspective differs from defensive or reactive methods because it highlights diplomacy's active function in creating digital norms.

Digital transformation scholars have sought to understand its impact on diplomatic roles and embassy functions. Foreign ministries across the world are modifying their core responsibilities because of cyber threats. The U.S. Department of State's Bureau of Cyberspace and Digital Policy together with the European Union's Cyber Diplomacy Toolbox demonstrate institutional approaches to diplomatic digital governance.[323] Embassies now function as forward-operating platforms for cyber diplomacy through their responsibility to monitor threats and advocate multilaterally and engage with technology firms and civil society. The Global Commission on the Stability of Cyberspace (2017–2019) shows that norm-building in cyberspace depends heavily on diplomatic collaboration between state and non-state actors.[324]

The diplomatic evolution faces increasing complexity according to the literature because emerging technologies especially Artificial Intelligence introduce new layers of complexity. According to Dinu and

---

[321] Ayman Attatfa, Lyes Khelladi, and Mohamed Amine Boudia, "Cyber Diplomacy: A Systematic Literature Review," *International Journal of Cyber Diplomacy* 1 (2020): 1–16.

[322] André Barrinha and Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, no. 4–5 (2017): 353–364.

[323] Annegret Bendiek, *The EU as a Force for Peace in International Cyber Diplomacy*, SWP Comment no. 19 (Berlin: Stiftung Wissenschaft und Politik, 2018), and Carmen-Elena Cîrnu, Carmen-Ionela Rotună, and Ioana-Cristina Vasiloiu, "Comparative Analysis on Cyber Diplomacy in EU and US," *Romanian Cyber Security Journal* 5, no. 1 (2023): 77–86.

[324] See Global Commission on the Stability of Cyberspace, *Advancing Cyberstability: Final Report*, November 2019, https://cyberstability.org/report.

Radanliev, AI creates problems regarding transparency and ethical regulation and attribution.[325] The issues require diplomatic involvement to actively address both AI deployment and its governance framework. AI functions as a tool that enables diplomatic practice, while simultaneously becoming a subject of international regulatory attention.

Bjola introduces the concept of "cognitive augmentation," which refers to AI's ability to support diplomatic decision-making under complexity and uncertainty. He then proposes the SIIT model — Strategic Intent, Innovation, Integration, and Transformation — to describe how foreign ministries can strategically embed AI into their operations.[326] This approach moves beyond reactive adaptation, signaling a long-term realignment of diplomatic roles and capabilities.

Stoltz extends the discussion by analyzing the United States' use of artificial intelligence in diplomatic activities. The author presents advantages of improved foresight and agility but identifies algorithmic bias and surveillance practices and diminished accountability as potential risks.[327] The criticisms match other international relations concerns about autonomy, human oversight and digital sovereignty.

The literature demonstrates that cyber diplomacy involves more than operational improvements because it drives changes in norms and institutions and geopolitical dynamics. AI integration forces diplomats to rethink their established procedures while requiring new approaches to global governance and role definitions and ethical responsibilities in the fast-evolving digital era.

---

[325] Mihaela Dinu, "Cyber Diplomacy and AI: Navigating Technological Ethics in International Relations," *Romanian Review of Political Sciences and International Relations* 20, no. 1 (2023): 77–91, and Stoyan Radanliev, "AI-Driven Cybersecurity and Risk Diplomacy in Global Conflict Response," *Journal of Cyber Risk and Diplomacy* 2, no. 1 (2025).

[326] Corneliu Bjola, "Diplomacy in the Age of Artificial Intelligence", *Emirates Diplomatic Academy Working Paper*, January 2020,

[327] William A. Stoltz, *Artificial Intelligence in Cybersecurity: Building Resilient Cyber Diplomacy Frameworks*, arXiv preprint, November 17, 2024.

Theoretical Framework

This research draws on Constructivism, Liberal Institutionalism, and Institutional Adaptation Theory to examine how Artificial Intelligence is reshaping the structures and operations of cyber diplomacy. Each theoretical lens offers a distinct perspective on this transformation: Constructivism emphasizes the discursive and normative dimensions of AI integration; Liberal Institutionalism highlights the role of international cooperation and governance frameworks; and Institutional Adaptation Theory focuses on how diplomatic institutions evolve and reorganize in response to technological change.

Through the constructivist perspective we can study the conceptual foundations of cyber diplomacy. International politics develops from material interests alongside norms and identities and shared meanings. AI receives its social construction through diplomatic discourse because multilateral settings become the site where risks and capabilities and ethical considerations are framed and contested and negotiated. According to Barrinha and Renard cyber diplomacy creates a new normative order which they call cyber-international society through which behavior norms emerge from interactive persuasion processes.[328]

Hodžić also supports this perspective by presenting diplomacy in the cyber realm as a process of identity negotiation which is characterized by ambiguity and shifting meanings.[329] The EU's focus on "trustworthy AI" and China's promotion of cyber sovereignty demonstrate how different cultural perspectives shape visions of future technology.[330] The way states imagine their future shapes their diplomatic approaches and foreign policy actions which demonstrate that AI functions beyond being a tool of power to shape global order.

---

[328] André Barrinha and Thomas Renard, "Cyber-Diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, no. 4–5 (2017): 353–364.

[329] Nejra Hodžić, *Cyber-Diplomacy: Framing the Transformation* (Master's thesis, Central European University, 2017), https://www.etd.ceu.edu/2017/hodzic_nejra.pdf.

[330] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2016).

Constructivism offers methods to study the development and spread of AI-related norms including transparency and accountability and human oversight. According to Finnemore and Sikkink norm internalization occurs through framing and persuasion and socialization which makes diplomatic discourse essential for technological governance.[331]

Liberal Institutionalism complements this perspective by showing how international organizations create conditions for cooperation and reduce uncertainty. The United Nations together with the European Union and OECD operate as platforms which promote norm diffusion and policy coordination and conflict resolution in cyberspace.[332] The establishment of AI-related standards and cyber confidence-building initiatives by these institutions demonstrates how diplomacy functions as a global governance instrument.

This tradition emphasizes that regimes along with rule-based mechanisms must address complex interdependence particularly in cybersecurity and AI ethics because unilateral action proves insufficient. The work of Keohane and Nye about complex interdependence continues to be relevant because multilateral forums have become essential for stabilizing expectations and building trust and knowledge sharing in cyber diplomacy.[333]

The Institutional Adaptation Theory examines internal organizational and bureaucratic changes needed for effective diplomatic relations with AI. Foreign Affairs ministries and embassies transform their responsibilities while moving resources and developing new capabilities to address technological disruptions. The creation of specialized roles including *cyber envoys*, *AI attachés* and *tech diplomats* demonstrates an organizational transformation toward digital diplomatic capabilities.[334]

---

[331] Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change," *International Organization* 52, no. 4 (1998): 887–917, https://doi.org/10.1162/002081898550789.

[332] Rebecca Devitt, "Liberal Institutionalism: An Alternative IR Theory or Just Maintaining the Status Quo?" *E-International Relations*, September 1, 2011.

[333] Robert O. Keohane and Joseph S. Nye, *Power and Interdependence: World Politics in Transition* (Boston: Little, Brown, 1977).

[334] Hocking, Brian, and Jan Melissen. *Diplomacy in the Digital Age: Evolution or Revolution?* Clingendael Institute, 2015.

March and Olsen suggest that institutional transformation emerges from historical backgrounds together with organizational work environments instead of logical planning approaches.[335] The adoption of AI technology occurs through a process that involves both uncertainty and ethical conflicts as well as international power struggles. The theory explains why particular states excel at AI diplomacy while others stay limited by organizational resistance and unclear policies.

These theories create a comprehensive analytical framework when combined together. Constructivism explains how ideas and identities shape AI discourse; Liberal Institutionalism accounts for the structures of global cooperation; and Institutional Adaptation Theory reveals how diplomatic institutions respond to technological transformation. The combined framework allows researchers to study cyber diplomacy through both its normative foundations and its institutional development.

Methodology

The research uses qualitative interpretive methods which draw from Constructivism Liberal Institutionalism and Institutional Adaptation Theory. The research aims to develop theoretical understanding about how Artificial Intelligence (AI) transforms cyber diplomacy while changing diplomatic roles and embassy functions in the modern digital global system. The interpretive research method proves most appropriate for this investigation because it focuses on meaning construction and institutional development and norm development which aligns with the theoretical framework.

The research bases its findings on a comparative analysis of the European Union together with the United States and China. The selected cases represent major diplomatic powers which implement different

[335] James G. March and Johan P. Olsen, "Institutional Perspectives on Political Institutions," *Governance* 9, no. 3 (1996): 247–264, https://doi.org/10.1111/j.1468-0491.1996.tb00242.x.

AI governance approaches through EU regulatory multilateralism and US strategic innovation and Chinese sovereignty-focused statecraft. The most different systems design (MDSD) framework enables researchers to detect common patterns and specific institutional and diplomatic differences between cases.[336]

The research depends mainly on document analysis of publicly accessible materials which includes the EU's Artificial Intelligence Act, the U.S. Cyber Diplomacy Act and United Nations Open-Ended Working Group (OEWG) proceedings.[337] The research incorporates scholarly publications together with institutional white papers and practitioner commentary to supplement the document analysis. All documents are analyzed to identify how AI was presented along with institutional arrangements and norm promotion methods in cyber diplomacy.

This analysis identifies empirical patterns including role redefinition and institutional restructuring and normative contestation which the selected theories help to interpret. The research focuses on understanding how AI-related diplomatic practices develop into institutionalized practices rather than seeking universal causal explanations.

This research faced several limitations stemming from its reliance on interpretive methods. By focusing primarily on official policy statements and institutional communications, it offers insights into discursive representations rather than the lived practices or personal experiences of diplomats. Moreover, the analysis centers on state actors, omitting the roles of private-sector innovators and civil society in shaping global AI diplomacy.

---

[336] Carsten Anckar, "The Most Similar- and Most Different Systems Design in Comparative Policy Analysis," in *Handbook of Research Methods and Applications in Comparative Policy Analysis*, eds. Guy Peters and Guillaume Fontaine (Cheltenham, UK: Edward Elgar Publishing, 2020), 33–48.

[337] European Union, *Artificial Intelligence Act*, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, *Official Journal of the European Union* L 2024/1689, July 12, 2024, https://eur-lex.europa.eu/eli/reg/2024/1689/oj; U.S. Congress, *Cyber Diplomacy Act of 2021*, H.R. 1251, 117th Congress, passed by the House of Representatives on April 20, 2021, https://www.congress.gov/bill/117th-congress/house-bill/1251; United Nations, *Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025*, established by General Assembly resolution 75/240 (December 31, 2020), https://disarmament.unoda.org/open-ended-working-group.

Future research could address these gaps by incorporating interviews, ethnographic observation, and network analysis to enrich empirical depth and include non-state perspectives.

Comparative Diplomatic Approaches to AI and Cyber Diplomacy

This section examines how the European Union, together with the United States and China, implement AI within their cyber diplomacy frameworks. The selection of these actors was based on their diplomatic significance and their unique institutional structures and different approaches to cyber governance. The analysis follows a Most Different Systems Design (MDSD) framework to understand how political cultures and normative frameworks influence AI engagement both as a diplomatic instrument and as a matter of global governance.

European Union: Normative Leadership

The EU demonstrates a rights-based cyber diplomacy framework which bases its operations on transparency and accountability and the rule of law. The EU demonstrates normative power through its *Artificial Intelligence Act* and *Cyber Diplomacy Toolbox* which extend its influence across international borders.[338] The EU's focus on "trustworthy AI" supports its mission to establish itself as a value-based global leader in digital governance.[339] The EU faces challenges in diplomatic action because its member states maintain different positions.

---

[338] European Commission, "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)," COM(2021) 206 final, Brussels, April 21, 2021, and Annegret Bendiek, *The EU as a Force for Peace in International Cyber Diplomacy*, SWP Research Paper 3 (Berlin: Stiftung Wissenschaft und Politik, 2018).

[339] Thomas Renard and André Barrinha, "Norm Entrepreneurship in Cyber Diplomacy: The EU's Cyber Diplomacy Toolbox," in *Cybersecurity and Diplomacy*, eds. Nicholas Burns and Jon Finer (Brussels: Egmont Institute, 2019), 97–116.

United States: Strategic Innovation and Alliances

The U.S. model focuses on technological leadership development while maintaining flexible governance approaches. The model supports a governance structure that brings together industry representatives with civil society organizations and international organizations. The U.S. promotes voluntary norms through its *Bureau of Cyberspace and Digital Policy* and its participation in OECD and GPAI forums while maintaining a liberal regulatory ethos.[340] The U.S. government implements institutional innovations through the placement of *cyber envoys* and *technology officers* in diplomatic missions and modernized training programs for diplomats[341].

China: Sovereignty and AI Diplomacy

China operates under a sovereignty-first framework which extends national authority throughout cyberspace. The diplomatic approach of China focuses on maintaining centralized control of digital infrastructure while protecting national narratives and using AI technology for economic and strategic advancement[342]. Through its *Digital Silk Road* program and *Global AI Governance Initiative* and diplomatic participation in UN OEWG and G20 and BRICS and G77 forums China demonstrates its goal to establish global standards based on state-led governance and non-interference principles[343]. China functions as a governance model alternative to Western approaches by supporting non-Western approaches to AI ethics and data governance and sovereignty protection. The state-centric model of

---

[340] William A. Stoltz, *Artificial Intelligence in Cybersecurity: Building Resilient Cyber Diplomacy Frameworks*, arXiv preprint, November 17, 2024, and Joseph S. Nye, "Soft Power and Public Diplomacy Revisited," *The Hague Journal of Diplomacy* 14, no. 1–2 (2019): 7–20.

[341] U.S. Government Accountability Office (GAO), *Cyber Diplomacy: State Department Needs a Strategy to Improve Engagement and Address Challenges*, GAO-23-105563 (Washington, DC: GAO, 2023).

[342] Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2016).

[343] Bayu Maulana and Muhammad Fajar, "Cyber Diplomacy and Geopolitical Tensions: Normative Contestations in AI Governance," *Journal of International Affairs and Global Strategy* 14 (2023): 21–36.

AI norm diffusion demonstrates unity through institutional integration between technical and diplomatic bureaucracies.

The cases demonstrate completely different diplomatic structures together with distinct normative systems. The EU follows a legalistic multilateral approach, while the U.S. uses strategic alliances with flexible governance and China promotes digital sovereignty through centralized statecraft and south-south partnerships. The three actors understand AI's geopolitical significance, but they implement different global digital order frameworks and demonstrate varying institutional flexibility.

AI and the Evolving Nature of Diplomatic Practice

Diplomatic foundations experience change because of AI which affects international actor engagement together with negotiation approaches and influence projection. AI introduces revolutionary changes to diplomatic practices by reshaping existing diplomatic norms and organizational frameworks and institutional capabilities.

Bjola's descriptive–predictive–prescriptive analytics model explains AI's operational support function in enabling decision-making operations. The model shows how cognitive augmentation improves crisis diplomacy by enhancing both foresight capabilities and responsiveness.[344]This model supports Institutional Adaptation Theory even though it lacks theoretical status. Bjola specifically highlights descriptive analytics as a useful tool to decrease uncertainty during international crises. AI enables ministries of foreign affairs to identify important patterns in real time which helps them navigate the "fog of war" and make timely decisions in high-stakes situations.[345] The ability to organize and understand rapidly changing

[344] Corneliu Bjola, "Diplomacy in the Age of Artificial Intelligence", *Emirates Diplomatic Academy Working Paper*, January 2020,

[345] Corneliu Bjola, *Artificial Intelligence and Diplomatic Crisis Management: Addressing the 'Fog of War' Problem*, DigDiploROx Working Paper No. 6 (Oxford Digital Diplomacy Research Group, July 2022),

information systems demonstrates how AI enhances strategic adaptation during diplomatic crises.

Constructivist scholars view artificial intelligence as a multifaceted instrument which embodies multiple conflicting values. Different political perspectives about AI including the EU's "trustworthy AI" approach, China's digital sovereignty stance and U.S. innovation support create competing narratives that influence diplomatic activities and norm development in multilateral settings.[346] Different visions reveal basic political identities and governance philosophies as core elements.

The implementation of AI technology in consular operations progresses through visa automation systems as well as fraud detection systems and diaspora outreach programs which allows efficient processing of large numbers of tasks.[347] The ministries of foreign affairs (MFAs) establish new positions including *cyber envoys*, *digital attachés* and *tech officers* while their staff receives training about AI ethics and cybersecurity.[348] The structural transformation showcases the predicted organizational changes according to Institutional Adaptation Theory.

Some governments have appointed "digital ambassadors" to directly work with Microsoft and Google among other major technology companies according to Konovalova.[349] Embassies operate today as private sector intermediaries to facilitate connections between states and transnational digital platforms through diplomatic arrangements.

---

[346] Thomas Renard and André Barrinha, "Norm Entrepreneurship in Cyber Diplomacy: The EU's Cyber Diplomacy Toolbox," in *Cybersecurity and Diplomacy*, edited by Nicholas Burns and Jon Finer, 97–116 (Brussels: Egmont Institute, 2019); Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age* (New York: PublicAffairs, 2016); William A. Stoltz, *Artificial Intelligence in Cybersecurity: Building Resilient Cyber Diplomacy Frameworks*, arXiv preprint, November 17, 2024,

[347] Zahra Mostafaei, Reza Karami, and Samira Khosravi, "Applications of Artificial Intelligence in Global Diplomacy," *Diplomacy & Technology Review* 4, no. 1 (2025): 33–47.

[348] U.S. Government Accountability Office (GAO), *Cyber Diplomacy: State Department Needs a Strategy to Improve Engagement and Address Challenges*, GAO-23-105563 (Washington, DC: GAO, 2023), https://www.gao.gov/products/gao-23-105563.

[349] Marta Konovalova, "AI and Diplomacy: Challenges and Opportunities," *Journal of Liberty and International Affairs* 9, no. 2 (2023): 520–530.

Generative AI tools including ChatGPT and DALL·E enable diplomatic operations to generate documents, translate information and conduct public outreach activities.[350] The deployment of these tools introduces three critical dangers which include hallucinated content,[351] protocol erosion[352] and misinformation.[353] Bano et al. and Zahid emphasize Human-in-the-loop safeguards have become essential because they protect quality standards and ensure contextual understanding and ethical oversight.[354]

AI systems should function as tools to enhance human judgment rather than replace it. According to Vacarelu and Zahid no algorithm exists that can duplicate the normative reasoning, cultural nuance, and empathy needed for diplomatic engagements.[355] Human decision authority needs to be preserved because it ensures accountability and maintains legitimacy.

The unequal distribution of AI capabilities between nations strengthens existing global inequalities. The development of technological leadership

---

[350] Corneliu Bjola, *Diplomacy in the Age of Artificial Intelligence*, Emirates Diplomatic Academy Working Paper (Abu Dhabi: EDA, 2020); Marius Vacarelu, "Artificial Intelligence: To Strengthen or to Replace Traditional Diplomacy?" in *Artificial Intelligence and Digital Diplomacy: Challenges and Opportunities*, edited by Fatima Roumate, 1–18 (Cham: Springer, 2021).

[351] The term hallucinated content describes AI-generated outputs which seem authentic but contain false information or made-up content. Maarten Sap et al. published "Neural False Narratives: Hallucinations in Language Models" in Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (2022) pages 135–146.

[352] The informal communication produced by AI technology leads to a breakdown of formal diplomatic procedures which researchers call protocol erosion. The article "Applications of Artificial Intelligence in Global Diplomacy" by Zahra Mostafaei, Reza Karami and Samira Khosravi appears in Diplomacy & Technology Review 4, no. 1 (2025) starting on page 33 and ending on page 47.

[353] The intentional sharing of false or misleading information constitutes misinformation. The American Psychological Association defines misinformation and disinformation through their website which can be accessed at https://www.apa.org/topics/journalism-facts/misinformation-disinformation on May 18, 2025.

[354] Sofia Bano, Daniel Baldino, and Andrea Deplano, "The Role of Generative AI in Global Diplomatic Practices," *Global Affairs* (2023); Fatima Binte Zahid, "Negotiating New Realities: Navigating the Intersection of Artificial Intelligence and Digital Diplomacy," *Internationale Politik Quarterly*, 2023.

[355] Marius Vacarelu, "Artificial Intelligence: To Strengthen or to Replace Traditional Diplomacy?" in *Artificial Intelligence and Digital Diplomacy: Challenges and Opportunities*, ed. Fatima Roumate (Cham: Springer, 2021), 1–18; Fatima Binte Zahid, "Negotiating New Realities: Navigating the Intersection of Artificial Intelligence and Digital Diplomacy," *Internationale Politik Quarterly*, 2023.

creates diplomatic advantages which push less-developed states toward marginalization in digital governance forums.[356] The process of establishing fair norms and inclusive participation becomes problematic because of these concerns.

Liberal Institutionalism explains how global platforms such as the OEWG, GPAI, and OECD attempt to harmonize AI norms. These platforms provide spaces for dialogue but their effectiveness is challenged by fragmented participation along with geopolitical rivalries that intensify due to uneven AI capabilities.

Institutional Adaptation Theory argues diplomatic reforms differ in their pace and depth of implementation. The early adoption of AI capabilities defines adaptive states but organizational inertia and strategic ambiguity restrict other countries from adopting AI-based solutions. Hocking and Melissen conclude that diplomatic resilience depends on institutional learning and flexibility together with strategic leadership that supports technological advancement.[357]

AI transforming diplomacy by introducing novel operational tools and by driving fundamental shifts in diplomatic practice, governance structures, and institutional frameworks. Through the reconfiguration of strategic capabilities and the establishment of new global standards, AI disrupts existing power hierarchies, fostering institutional innovation and intensifying normative debates in international relations.

Policy Recommendations

To ensure cyber diplomacy remains an effective and responsible tool of global governance in the AI era, the following policy actions are recommended:

---

[356] Joseph S. Nye, "The End of Anarchy? How to Build a New Digital Order," *Foreign Affairs* 100, no. 6 (2021): 111–120.

[357] Brian Hocking and Jan Melissen, *Diplomacy in the Digital Age* (The Hague: Clingendael Institute, 2015).

1. Integrate AI ethics and governance into diplomatic training programs.
2. Establish global standards for generative AI through inclusive multilateral platforms.
3. Empower Global South participation in shaping AI governance norms and frameworks.
4. Appoint AI attachés and technology envoys within diplomatic institutions.
5. Mandate transparent, human-in-the-loop frameworks for AI system deployment.
6. Facilitate continuous dialogue between governments, private tech firms, and civil society.

Conclusion

The emergence of artificial intelligence has propelled cyber diplomacy from a peripheral concern to a central pillar of international relations. As AI technologies reshape how diplomacy is conducted, they also redefine the institutions, values, and power dynamics that underpin global governance. This paper has shown that AI's impact on diplomacy unfolds through three interrelated processes: technological disruption, institutional adaptation, and normative contestation.

Using a Constructivist lens, the analysis illustrated how competing narratives — such as democratic openness versus digital sovereignty — shape the strategic use of AI by major actors like the EU, the U.S., and China. Liberal Institutionalism helped illuminate the dual role of international organizations in facilitating cooperation while struggling to maintain governance coherence. Institutional Adaptation Theory further revealed how foreign ministries are evolving their structures, mandates, and competencies in response to AI's rapid advancement.

The study also drew on emerging frameworks and empirical studies to underscore AI's practical implications — from real-time decision support in crisis diplomacy to the risks of generative content and the growing involvement of non-state actors. These developments demonstrate both

the promise and peril of AI-driven diplomacy. The descriptive–predictive–prescriptive analytics model developed by Bjola shows how AI decreases uncertainty while improving cognitive performance in crisis diplomacy through real-time situational awareness and decision support for diplomats. The SIIT model presents a strategic framework to integrate AI into institutional frameworks through structural modifications. The introduction of generative AI tools including ChatGPT and DALL·E extends content diplomacy capabilities yet introduces risks which include fabricated outputs and false information and violations of diplomatic protocols. The development of virtual embassies alongside bilateral relations with major technology companies demonstrates that institutional adaptation now encompasses non-state digital actors. The research by Mostafaei et al. proves AI's expanding utility in consular work through visa automation and fraud detection systems which demonstrate its value beyond strategic operations.

Crucially, the future of cyber diplomacy hinges not just on technological capacity, but on ethical reflexivity. Diplomats must not only deploy AI strategically but guide its development through inclusive, accountable, and norm-based engagement. Their ability to do so will help determine whether AI becomes a force for global cooperation — or a driver of digital fragmentation.

Bibliography

Bano, Sofia, Daniel Baldino, and Andrea Deplano. "The Role of Generative AI in Global Diplomatic Practices." *Global Affairs*, 2023.

Barrinha, André, and Thomas Renard. "Cyber-Diplomacy: The Making of an International Society in the Digital Age." *Global Affairs* 3, no. 4–5 (2017): 353–364.

Bendiek, Annegret. *The EU as a Force for Peace in International Cyber Diplomacy*. SWP Research Paper 3. Berlin: Stiftung Wissenschaft und Politik, 2018.

Bjola, Corneliu. "Diplomacy in the Age of Artificial Intelligence." Emirates Diplomatic Academy Working Paper, 2020.

Bjola, Corneliu. "Artificial Intelligence and Diplomatic Crisis Management." *AI Diplomacy Series*, Oxford Digital Diplomacy Research Group, 2022.

Cîrnu, Daniel, et al. "Comparative Analysis on Cyber Diplomacy in the EU and US." *Journal of Strategic and International Studies*, 2023.

Dinu, Mihaela. "Cyber Diplomacy and AI: Navigating Technological Ethics in International Relations." *Romanian Review of Political Sciences and International Relations* 20, no. 1 (2023): 77–91.

European Commission. "Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." COM(2021) 206 final. Brussels, 2021.

GAO (U.S. Government Accountability Office). *Cyber Diplomacy: State Department Needs a Strategy to Improve Engagement and Address Challenges*. GAO-23-105563. Washington, DC, 2023.

Hodžić, Nejra. "Cyber-Diplomacy: Framing the Transformation." MA Thesis, Central European University, 2017.

Hocking, Brian, and Jan Melissen. *Diplomacy in the Digital Age*. The Hague: Clingendael Institute, 2015.

Konovalova, Marta. "AI and Diplomacy: Challenges and Opportunities." *Journal of Liberty and International Affairs* 9, no. 2 (2023): 520–530.

Maulana, Bayu, and Muhammad Fajar. "Cyber Diplomacy and Geopolitical Tensions: Normative Contestations in AI Governance." *Journal of International Affairs and Global Strategy* 14 (2023): 21–36.

Manners, Ian. "Normative Power Europe: A Contradiction in Terms?" *Journal of Common Market Studies* 40, no. 2 (2002): 235–258.

Mostafaei, Zahra, et al. "Applications of Artificial Intelligence in Global Diplomacy." *Diplomacy & Technology Review* 4, no. 1 (2025): 33–47.

Nye, Joseph S. "Soft Power and Public Diplomacy Revisited." *The Hague Journal of Diplomacy* 14, no. 1–2 (2019): 7–20.

Renard, Thomas, and André Barrinha. "Norm Entrepreneurship in Cyber Diplomacy: The EU's Cyber Diplomacy Toolbox." In *Cybersecurity and Diplomacy*, edited by Nicholas Burns and Jon Finer, 97–116. Brussels: Egmont Institute, 2019.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York: PublicAffairs, 2016.

Stoltz, Mitchell. "AI and Automation in US Cyber Diplomacy." *arXiv preprint* arXiv: 2411.13585 (2024).

Vacarelu, Marius. "Artificial Intelligence: To Strengthen or to Replace Traditional Diplomacy?" In *Artificial Intelligence and Digital Diplomacy: Challenges and Opportunities*, edited by Fatima Roumate, 1–18. Cham: Springer, 2021.

Zahid, Fatima Binte. "Negotiating New Realities: Navigating the Intersection of Artificial Intelligence and Digital Diplomacy." *Internationale Politik Quarterly*, 2023.

2

Cameras in the Sky: A Summary of How Unmanned Aerial Vehicles Continue to Change how Conflicts are Fought Since 2008

Alexander MOCK

Abstract: This report analyzes the evolving impact of drones on military strategy and policy through three case studies from conflicts in Eastern Europe. It examines how unmanned aerial vehicles (UAVs) have influenced infantry tactics and armored warfare, drawing on sources such as the U.S. Department of Defense's UAV roadmap (2000–2025), recent advancements in AI-driven drone technology, and assessments of how mass drone strikes undermine air defense systems. These findings are contextualized within the broader security risks facing U.S. military installations in the Middle East. The report concludes by recommending increased investment in electromagnetic pulse (EMP) weapons as a viable countermeasure to enhance base defense and mitigate the threat of drone-based attacks.

Keywords: asymmetric warfare, hybrid threat theory, soft power, hard power, artificial intelligence

Introduction

As drone technology advances, its impact on warfare strategy has moved from experimental to essential, transforming both offensive tactics and defensive planning. This paper focuses on conflicts in Eastern Europe since 2008, specifically the Russo-Georgian War and the ongoing Russo-Ukrainian War, to analyze the role of drones in shaping modern warfare.

Using a comparative case study approach, this paper focuses on the 2008 Russo-Georgian War and the ongoing 2022–2025 Russo-Ukrainian War. It draws on government reports, tactical assessments, and open-source intelligence to trace how UAV capabilities have evolved and what impact they've had on the battlefield. A key limitation of this paper is its reliance on publicly available, open-source intelligence concerning a dynamic, ongoing conflict, where data is often difficult to verify and may be subject to the influence of wartime propaganda.

This paper explores the use of artificial intelligence in drones, along with the potential risks such technologies pose. It also considers how the ongoing Russo-Ukrainian conflict might influence future drone operations by terrorist groups targeting U.S. bases in the Middle East. To address these threats, the United States should invest in the development and deployment of electromagnetic pulse (EMP) and high-power microwave (HPM) weapons as effective countermeasures against drone incursions and swarm attacks.

The analysis concludes by providing policy proposals to further invest in the development and deployment of EMP and HPM weapons to counter future drone incursions and assaults.

Military Applications of UAVs

While each country's military uses UAVs differently, this section focuses on five key methods of employing these systems in modern combat.[358]

[358] Cook, Kendra L. "The silent force multiplier: The history and role of uavs in warfare." *2007 IEEE Aerospace Conference*, 2007, pp. 1, https://doi.org/10.1109/aero.2007.352737.

Larger UAVs, such as the MQ-9 Reaper series produced by General Atomics, are equipped with powerful fire-and-forget missiles capable of targeting both armored vehicles and personnel.[359] However, these drones are large and expensive to operate and maintain. For example, a new MQ-9 Reaper costs roughly $30 million. Countries with smaller defence budgets may not have the resources to build or acquire such expensive equipment. Smaller quadcopter craft, such as the Chinese built DJI, has been used extensively in Ukraine.[360] Its small size and cheap cost of around $400 per unit on Amazon allows countries with smaller budgets to provide an effective and affordable drone for their armed forces. Comparable commercially available vehicles can be modified to carry infrared cameras for reconnaissance, if such capabilities are not already pre-installed by the manufacturer. Other alterations may include attaching improvised bomb bays to drop on soldiers or armored vehicles.[361] Commercial drones are also a more cost effective alternative which produces similar results, although ideal outcomes are less reliable to achieve due to the crude customizations retrofitted onto the craft.

Drones are also used for psychological warfare, such as intentionally hovering a UAV over enemy combatants. This tactic can force soldiers to abandon advantageous or concealed positions out of fear of an air-dropped grenade or having their location relayed to nearby units.[362] Prolonged exposure also degrades the morale of an adversary and induces paranoia, both of which negatively impact everyday motor functions and combat performance.[363] Furthermore, trained drone operators carry

---

[359] U.S. Air Force. "MQ-9 Reaper." U.S. Air Force, September 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper.

[360] Franke, Ulrike. "Drones in Ukraine: Four Lessons for the West." ECFR. European Council on Foreign Relations (ECFR), January 10, 2025. https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west.

[361] Franke, Ulrike. "Drones in Ukraine and Beyond: Everything You Need to Know." *European Council on Foreign Relations*, August 11, 2023. https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know.

[362] Hijazi, Alaa, Christopher J. Ferguson, F. Richard Ferraro, Harold Hall, Mark Hovee, and Sherrie Wilcox. "Psychological Dimensions of Drone Warfare." *Current Psychology* 38, no. 5 (September 14, 2017): 1285–96. https://doi.org/10.1007/s12144-017-9684-7.

[363] Holz, Jacob. "Victimhood and Trauma within Drone Warfare." *Critical Military Studies* 9, no. 2 (July 29, 2021): 1–16. https://doi.org/10.1080/23337486.2021.1953738.

little risk of being spotted, as the operator can sit several thousands of miles away from his or her target.[364] Other frontline platoon-level units may operate small unmanned aerial systems (SUAVs), similar in size to the RQ-11 Raven. One key advantage of the Raven is that it's compact enough to be hand-launched by a single infantryman for immediate area reconnaissance.[365] This permits real time battlefield data to flow from a platoon on the field to commissioned officers for enhanced situational awareness.[366]

The introduction of Unmanned Aerial Systems allows the elimination of such attacks without expending considerable amounts of ammunition and other essential resources. Brainstorming methods to counter possible attacks is made much easier with the ongoing conflict in Ukraine and its abundance of combat footage circulating online.[367] The U.S. needs to take advantage of these recordings and after action reports in order to address potential flaws currently present in UAV policy, capability, and effective counter strategy.[368] Furthermore, the entire United States military apparatus should increase spending on drone technology and development in order to maintain its lead in UAS systems.[369]

---

[364] Jeangène Vilmer, Jean-Baptiste. "Not so Remote Drone Warfare." *International Politics* 60 (July 22, 2021): 898. https://doi.org/10.1057/s41311-021-00338-9.

[365] Jeffery, Capt, Van Bourgondien, David Matthews, and Raymond Franck. "Analysis of the Sustainment Organization and Process for the Marine Corps' RQ-11B Raven Small Unmanned Aircraft System (SUAS)," 2012. https://www.dair.nps.edu/bitstream/123456789/2031/1/NPS-LM-12-010.pdf.

[366] Mahadevan. "The Military Utility of Drones." *ETH Zurich*, no. 78 (July 2010), 2–4. https://doi.org/10.3929/ethz-a-006253833.

[367] On Demand News. "Intense Combat Footage Shows Mercenaries Fighting in Ukraine-Russia War | Full Series." YouTube, April 12, 2025. https://www.youtube.com/watch?v=pclT0pngf_k.

[368] Guitton, Matthieu J. "Fighting the Locusts: Implementing Military Countermeasures against Drones and Drone Swarms." *Scandinavian Journal of Military Studies* 4, no. 1 (2021): 30–33. https://doi.org/10.31374/sjms.53.

[369] Hlotov, V., A. Hunina, S. Kniaziev, V. Kolesnichenko, and O. Prokhorchuk. "Analysis of Application of the UAVs for Military Tasks." *Modern Achievements of Geodesic Science and Industry* I, no. 37 (2019): 69–77. https://doi.org/10.33841/1819-1339-2019-1-37-69-77.

Unmanned Aerial Systems in the 2008 Russo Georgian War

In the years leading up to the short six day conflict, Georgia had feuded with Moscow with its aspirations of joining the North Atlantic Treaty Organization.[370] In what has become a running theme since then, Putin supplied arms and ammunition to those provinces in which Georgians were publicly pro-Kremlin and did not want to become a part of NATO.[371] Following the loss of two Georgian UAVs by pro-Russian separatists, Russian president Vladimir Putin launched an invasion of Georgia in early August of 2008.[372] The size of the Georgian Army and its allies were far smaller at roughly 12,000, men compared to Russia's 23,000.[373] However, they held a slight strategic advantage due to owning about 40 units of the Elbit Systems *Hermes 450* surveillance drone, which were bought from Israel prior to the conflict.[374] Produced since 1998, the *Hermes* drone possesses several advanced features. These include payload options of a ground moving target indication array, radar with track while scan capabilities, and endurance of up to 17 hours.[375] Deploying these unmanned systems permitted Georgian units to track Russian personnel and armored vehicles with significantly decreased risk to their own safety. The *Hermes* system also allowed for more accurate artillery fire

---

[370] Clayton, Nicholas. "How Russia and Georgia's 'Little War' Started a Drone Arms Race — the World from PRX." The World from PRX, July 31, 2016. https://theworld.org/stories/2016/07/31/how-russia-and-georgias-little-war-started-drone-arms-race.

[371] Clayton, Nicholas. "How Russia and Georgia Started a Drone Arms Race." Anchorage Daily News, May 13, 2016. https://www.adn.com/nation-world/article/how-russia-and-georgia-started-drone-arms-race/2012/10/23.

[372] Peter Dickinson. "Abkhazia Claims Shootdown of 2 Georgian Spy Drones." Voice of America. Voice of America (VOA News), October 27, 2009. https://www.voanews.com/a/a-13-2008-05-04-voa21-66646552/557338.html.

[373] Kofman, Michael. "Russian Performance in the Russo-Georgian War Revisited." War on the Rocks, September 4, 2018. https://warontherocks.com/2018/09/russian-performance-in-the-russo-georgian-war-revisited.

[374] Gettinger, Dan. "'Drones Are Not Toys': The Russian Program." Bard.edu, March 5, 2014. https://dronecenter.bard.edu/drones-toys-russian.

[375] Army.mil. "ODIN — OE Data Integration Network." ODIN, 2025. https://odin.tradoc.army.mil/WEG/Asset/64d41728a7da9861432867e4a4fcef05.

on designated targets with the assistance of spotters, GPS tracking, and rangefinding lasers.[376]

In comparison, Russia's drone infrastructure was negligible at best when war broke out.[377] Unmanned aerial units were limited to the *Pchela-1T* (Bee-1), which were tested in 1987 and adopted in 1990 by the Yakovlev Design Bureau.[378] These aircraft were responsible for providing battlefield intelligence back to the Russians; however, there were several limitations with the *Pchela*. For example, it was launched using two rocket boosters without sound suppression equipment.[379] This would allow the sound waves to be picked up by loitering *Hermes* drones; consequently compromising the drones' position and flight path to be intercepted and shot down using rifles or surface to air missiles.[380] Other disadvantages included a short endurance time of about 2 hours, minimal service life, and outside of reporting target acquisition, possessed very few advanced electronic systems.[381] This lack of reliable UAV systems led to the necessity of deploying manned Sukhoi SU-24 MR "Fencer-E" supersonic reconnaissance aircraft in order to designate vital targets and detect troop movements.[382]

In the aftermath of the Russo Georgian conflict, Russia would publicly announce a desire to heavily invest in increasing their drone

---

[376] Ghadir Hamadi. "What You Need to Know about the $2 Million Israeli Drone Hezbollah Shot down Yesterday." L'Orient Today, February 26, 2024. https://today.lorientlejour.com/article/1369444/what-you-need-to-know-about-the-2-million-israeli-drone-hezbollah-shot-down-today.html.

[377] Gettinger, Dan. "'Drones Are Not Toys': The Russian Program." Bard.edu, March 5, 2014. https://dronecenter.bard.edu/drones-toys-russian.

[378] Luzin, Pavel. "RUSSIAN MILITARY DRONES Past, Present, and Future of the UAV Industry," November 2023. https://www.fpri.org/wp-content/uploads/2023/11/russian-military-drones-.pdf.

[379] Bongo. "Domestic Unmanned Aircraft (Part 3)." Военное обозрение, March 14, 2018. https://en.topwar.ru/137596-otechestvennaya-bespilotnaya-aviaciya-chast-3.html.

[380] McDermott, Roger. "Russia's UAVs and UCAVs: ISR and Future Strike Capabilities." Jamestown, March 23, 2022. https://jamestown.org/program/russias-uavs-and-ucavs-isr-and-future-strike-capabilities.

[381] Army.mil. "ODIN — OE Data Integration Network," 2025. https://odin.tradoc.army.mil/Search/WEG/pchela.

[382] "Sukhoi Su-24 — Archived 3/2003." Sukhoi Su-24 — Archived 3/2003. Accessed July 3, 2025. https://www.forecastinternational.com/archive/disp_old_pdf.cfm?ARC_ID=1047.

capability.[383] However, economic sanctions were imposed by the United States and the European Union in the aftermath of the annexation of Crimea in 2014.[384] As a result, Russia was forced to rely on imported drones and their parts from countries such as Iran and China.[385] This was achieved through the informal founding of BRICS in 2006 and formal founding in 2009.[386] The forming of the alliance permitted Russia to bypass some of the sanctions to trade with non NATO members which have become increasingly opposed to the West.[387] In the aftermath of Russia's invasion of Ukraine, five new members have been accepted into what has developed into a competitor with NATO.[388]

Unmanned Aerial Systems in Ukraine from 2022 to mid 2025

Considering Ukraine and Georgia's proximity to Russia, it was only a matter of when Putin would decide to invade Ukraine next.[389] On the February 24, 2022, President Vladimir Putin ordered an illegal full scale invasion of

---

[383] Bučka, Pavel, Ján Marek, and Rudolf Pástor. "Modernization of the Armed Forces of the Russian Federation after the Russian-Georgian Conflict." *Politické vedy* 24, no. 2 (September 10, 2021): 68–70. https://doi.org/10.24040/politickevedy.2021.24.2.62-86.

[384] European Commission. "Sanctions Adopted Following Russia's Military Aggression against Ukraine." finance.ec.europa.eu, 2023. https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en.

[385] The Insider. "Four Rotors and a Prayer: How Russia Built a Billion-Ruble Drone Industry Using Chinese Parts." The Insider, May 16, 2025. https://theins.ru/en/inv/281354.

[386] Library of Congress. "Research Guides: BRICS: Sources of Information: Introduction." Loc.gov, 2016. https://guides.loc.gov/brics.

[387] Baunov, Alexander. "New Identity for BRICS." Carnegie Endowment for International Peace, 2024. https://carnegieendowment.org/russia-eurasia/politika/2024/10/brics-russia-global-power-opposition?lang=en.

[388] Patrick, Stewart, Erica Hogan, and Oliver Stuenkel. "BRICS Expansion and the Future of World Order: Perspectives from Member States, Partners, and Aspirants." Carnegie Endowment for International Peace, March 31, 2025. https://carnegieendowment.org/research/2025/03/brics-expansion-and-the-future-of-world-order-perspectives-from-member-states-partners-and-aspirants?lang=en.

[389] Beehner, Lionel, Liam Collins, Steve Ferenzi, Robert Person, and Aaron Brantly. "Analyzing the Russian Way of War Evidence from the 2008 Conflict with Georgia a Contemporary Battlefield Assessment by the Modern War Institute," 2018, 71. https://vtechworks.lib.vt.edu/server/api/core/bitstreams/808c5992-2f32-4f04-b339-eb9ba53064bd/content.

Ukraine.[390] Since then, the Russo Ukrainian War has largely become reminiscent of tactics deployed during World War One, with several hundred miles of trenches being constructed by both sides.[391] One of the primary weapons which have become synonymous with the conflict is the extensive employment of numerous unmanned aerial vehicles deployed by both Russia and Ukraine.[392] However, Russia's lack of infrastructure in order to produce their own drones due to western sanctions has forced the army to become reliant on imported models from Iran and China.[393]

For instance, as of mid June 2025, Russia has been consistently receiving drone shipments from Iran to assist in the war effort.[394] Iranian drones such as the Shahed-129 "Eye-Witness" produced by HESA have enhanced Russian combat capability and situational awareness, along with limited precision strike capability.[395] Another drone which has made some headlines include the Qasef-1, which is a loitering munition UAS also produced by HESA.[396] Shahid drones can be made with materials such as wood, and cost anywhere from $20,000 to $50,000 a piece.[397] These drones are used to fly around a combat area until a target is identified by the operator, after

---

[390] Center for Preventive Action. "War in Ukraine." Global Conflict Tracker. Council on Foreign Relations, May 27, 2025. https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine.

[391] Axe, David. "Ukrainian Troops Are Digging Trenches in Russia's Kursk Oblast. It's a Sign They Plan to Stay." *Forbes*, August 12, 2024. https://www.forbes.com/sites/davidaxe/2024/08/11/ukrainian-troops-are-digging-trenches-in-russias-kursk-oblast-its-a-sign-they-plan-to-stay.

[392] Dickinson, Peter. "Putin's Escalating Air Offensive Is Overwhelming Ukraine's Defenses." Atlantic Council, July 2025. https://www.atlanticcouncil.org/blogs/ukrainealert/putins-escalating-air-offensive-is-overwhelming-ukraines-defenses.

[393] Espreso TV. "French Aeronaut Explains Why Russian Army Is Unable to Use Drones Effectively." @Espresotveng. Espreso, May 9, 2023. https://global.espreso.tv/french-aeronaut-explains-why-russian-army-is-unable-to-use-drones-effectively.

[394] Eslami, Mohammad. "Iran's Drone Supply to Russia and Changing Dynamics of the Ukraine War." *Journal for Peace and Nuclear Disarmament* 5, no. 2 (November 20, 2022): 1–12. https://doi.org/10.1080/25751654.2022.2149077.

[395] Military Factory. "HESA Shahed-129 (Eye-Witness) Medium-Altitude, Long-Endurance (MALE) Reconnaissance / Light Attack Drone." Militaryfactory.com, July 13, 2022. https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=1330.

[396] Military Factory. "HESA Qasef-1 Loitering Munition / UCAV Drone." www.militaryfactory.com, June 22, 2022. https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2155.

[397] Jensen, Benjamin and Atalan, Yasir, p.2. "Drone Saturation: Russia's Shahed Campaign." CSIS Briefs, May 2025. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-05/250513_Jensen_Drone_Saturations.pdf?VersionId=QsQBXrKcuEpHw4yK0EoTr7ZIraS5yTMW.

which the craft is directed at the target and detonates using the explosive material in the nose upon impact.[398]

The Ukrainians' capabilities of producing its own domestic drones gives the Ukrainian Armed Forces one of the few advantages in its war with Russia.[399] Development and adoption of new drones since 2014 have been slow; however, New Geopolitics Research Network member Mykhailo Samus states "the UAF operated about 70 different types of unmanned aerial systems, as well as more than 20 types of ammunition for attack drones" during the end of 2023.[400]

Employment of Swarm Attacks

Both countries have developed swarm tactics to varying degrees of success against both strategic and non strategic targets.[401] For example, on June 1, 2025, Ukrainian special forces launched over 100 explosive laden drones to disable or destroy Russian strategic and nuclear bombers.[402] The aircraft which were targeted included Tupolev built TU-95 "*Bear*" and TU-22 "*Blinder"* bombers, along with Beriev A-50 "*Moss*" airborne early warning and control aircraft.[403] Due to Russian bomber doctrine, these aircraft were

---

[398] Atherton, Kelsey. "Loitering Munitions Preview the Autonomous Future of Warfare." Brookings, August 4, 2021. https://www.brookings.edu/articles/loitering-munitions-preview-the-autonomous-future-of-warfare.

[399] Axe, David. "4.5 Million Drones Is a Lot of Drones. It's Ukraine's Goal for 2025." Forbes, March 12, 2025. https://www.forbes.com/sites/davidaxe/2025/03/12/45-million-drones-is-a-lot-of-drones-its-ukraines-new-production-target-for-2025.

[400] Samus, Mykhailo. "Lessons-Learned-from-the-War-in-Ukraine.-the-Impact-Of-..." Lessons Learned From The War in Ukraine. The Impact of Drones, 2024, p.6. https://newstrategycenter.ro/wp-content/uploads/2024/02/Lessons-Learned-from-the-War-in-Ukraine.-The-impact-of-Drones-2.pdf.

[401] Deni Ellis Béchard. "How Drone Swarms Work—from Iran's Shahed Attack to Ukraine's Operation Spiderweb." Scientific American, June 16, 2025. https://www.scientificamerican.com/article/how-drone-swarms-work-from-irans-shahed-attack-to-ukraines-operation.

[402] Bondar, Kateryna. "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare." Csis.org, 2025. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.

[403] Deni Ellis Béchard. "How Drone Swarms Work—from Iran's Shahed Attack to Ukraine's Operation Spiderweb." Scientific American, June 16, 2025. https://www.scientificamerican.com/article/how-drone-swarms-work-from-irans-shahed-attack-to-ukraines-operation.

already carrying fuel and weapon loads for immediate deployment.[404] These aircraft were stationed in four bases without hangers or any kind of overhead protection.[405] During the attack, about 40 were damaged and the drones successfully "destroyed at least 13 [aircraft]."[406] These first person view drones were deployed from inside Russian territory by containing the drones in cargo containers and smuggling them across the border.[407] This allowed the drivers to control the trucks in complete anonymity, as Russian border guards would not have been able to tell what kind of payload was being transported.[408]

Policy Proposals

Due to the abundance of footage of drone attacks circulating on the internet, concern should be raised regarding when a terrorist organization decides to take inspiration from the war in Ukraine.[409] In order to combat these security threats, the United States military should continue to develop mobile High Power Microwaves, or HPMs, to disable drones and UAVs.[410] Such weapons could be used to great effect by U.S. bases stationed in the

[404] Maj, Philip, Stemple, Advisor Major, Thomas Meara, Maxwell Air, and Force Base. "THE SOVIET AIR FORCE and STRATEGIC BOMBING a Research Report Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements," 1999. https://apps.dtic.mil/sti/tr/pdf/ADA398859.pdf.

[405] Jenson, Benjamin. "American.edu." American University, 2025. https://www.american.edu/sis/news/20250605-ukraines-operation-spider-web-upended-traditional-rules-of-war.cfm.

[406] Dahlgren, Masao, and Lachlan MacKenzie. "Ukraine's Drone Swarms Are Destroying Russian Nuclear Bombers. What Happens Now?" Csis.org, 2025. https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now.

[407] Horowitz, Michael C. "Ukraine's Operation Spider's Web Shows Future of Drone Warfare." Council on Foreign Relations, June 3, 2025. https://www.cfr.org/expert-brief/ukraines-operation-spiders-web-shows-future-drone-warfare.

[408] Dahlgren, Masao, and Lachlan MacKenzie. "Ukraine's Drone Swarms Are Destroying Russian Nuclear Bombers. What Happens Now?" Csis.org, 2025. https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now.

[409] *BBC*. "Video Appears to Show Ukraine Drone Attack in Russia." June 1, 2025. https://www.bbc.com/news/videos/cvg53nyg72vo.

[410] Othman Dhari Razooqi, and Alaa H Ali. "Drones Neutralized by Utilize Electromagnetic Pulse (EMP) System." *2022 5th International Conference on Engineering Technology and Its Applications (IICETA)*, no. 1 (May 31, 2022): 487–88. https://doi.org/10.1109/iiceta54559.2022.9888673.

Middle East[411]. Although EMP devices can be developed, they would need to be fairly powerful- around 6 gigahertz- to create a noticeable impact on a drone's performance.[412] In the case of drone swarms, several of either of these devices would need to be present in order to disrupt communications with the controller.[413]

Conclusion

With expanded access to battlefield footage on the internet, terrorist and paramilitary organizations have a new blueprint to take influence from to attack U.S. bases overseas. In order to effectively counter these threats, our military needs to continue to keep a close eye on the conflicts currently playing out abroad. Analyzing drone attacks will introduce new challenges to overcome in our UAS development and counter drone strategy. Central to countering UAV concerns is the development and utilization of electromagnetic pulse and high power microwave weapons to disable the circuits of drones.

Bibliography

Atherton, Kelsey. "Loitering Munitions Preview the Autonomous Future of Warfare." *Brookings*, August 4, 2021. https://www.brookings.edu/articles/loitering-munitions-preview-the-autonomous-future-of-warfare.

Axe, David. "4.5 Million Drones Is a Lot of Drones. It's Ukraine's Goal for 2025." *Forbes*, March 12, 2025. https://www.forbes.com/sites/davidaxe/2025/03/12/45-million-drones-is-a-lot-of-drones-its-ukraines-new-production-target-for-2025.

---

411 Easter, Reagan. "U.S. Forces in the Middle East: Under Attack and Defending Israel." FDD, June 16, 2025. https://www.fdd.org/analysis/policy_briefs/2025/06/16/u-s-forces-in-the-middle-east-under-attack-and-defending-israel.

412 Razooqi, Othman Dhari, and Alaa. H. Ali. "Drones Neutralized by Utilize Electromagnetic Pulse (EMP) System." *2022 5th International Conference on Engineering Technology and its Applications (IICETA)*, May 31, 2022, 487–88. https://doi.org/10.1109/iiceta54559.2022.9888673.

413 Othman Dhari Razooqi, and Alaa H Ali. "Drones Neutralized by Utilize Electromagnetic Pulse (EMP) System." *2022 5th International Conference on Engineering Technology and Its Applications (IICETA)*, no. 1 (May 31, 2022): 489–90. https://doi.org/10.1109/iiceta54559.2022.9888673.

Axe, David. "Ukrainian Troops Are Digging Trenches in Russia's Kursk Oblast. It's a Sign They Plan to Stay." *Forbes*, August 12, 2024. https://www.forbes.com/sites/davidaxe/2024/08/11/ukrainian-troops-are-digging-trenches-in-russias-kursk-oblast-its-a-sign-they-plan-to-stay.

Baunov, Alexander. "New Identity for BRICS." *Carnegie Endowment for International Peace*, 2024. https://carnegieendowment.org/russia-eurasia/politika/2024/10/brics-russia-global-power-opposition?lang=en.

Beehner, Lionel, Liam Collins, Steve Ferenzi, Robert Person, and Aaron Brantly. *Analyzing the Russian Way of War: Evidence from the 2008 Conflict with Georgia — A Contemporary Battlefield Assessment by the Modern War Institute*. West Point, NY: Modern War Institute, 2018. https://vtechworks.lib.vt.edu/server/api/core/bitstreams/808c5992-2f32-4f04-b339-eb9ba53064bd/content.

Bongo. "Domestic Unmanned Aircraft (Part 3)." *Voennoe Obozrenie (Military Review)*, March 14, 2018. https://en.topwar.ru/137596-otechestvennaya-bespilotnaya-aviaciya-chast-3.html.

Bondar, Kateryna. "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare." *Center for Strategic and International Studies (CSIS)*, 2025. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare.

Bučka, Pavel, Ján Marek, and Rudolf Pástor. "Modernization of the Armed Forces of the Russian Federation after the Russian-Georgian Conflict." *Politické vedy* 24, no. 2 (September 10, 2021): 68–70. https://doi.org/10.24040/politickevedy.2021.24.2.62-86.

British Broadcasting Corporation. "Video Appears to Show Ukraine Drone Attack in Russia." *BBC News*, June 1, 2025. https://www.bbc.com/news/videos/cvg53nyg72vo.

Center for Preventive Action. "War in Ukraine." *Global Conflict Tracker*. Council on Foreign Relations, May 27, 2025. https://www.cfr.org/global-conflict-tracker/conflict/conflict-ukraine.

Clayton, Nicholas. "How Russia and Georgia Started a Drone Arms Race." *Anchorage Daily News*, May 13, 2016. https://www.adn.com/nation-world/article/how-russia-and-georgia-started-drone-arms-race/2012/10/23.

Clayton, Nicholas. "How Russia and Georgia's 'Little War' Started a Drone Arms Race." *The World from PRX*, July 31, 2016. https://theworld.org/stories/2016/07/31/how-russia-and-georgias-little-war-started-drone-arms-race.

Cook, Kendra L. "The Silent Force Multiplier: The History and Role of UAVs in Warfare." In *2007 IEEE Aerospace Conference*, 1–10. IEEE, 2007. https://doi.org/10.1109/aero.2007.352737.

Dahlgren, Masao, and Lachlan MacKenzie. "Ukraine's Drone Swarms Are Destroying Russian Nuclear Bombers. What Happens Now?" *Center for Strategic and International Studies (CSIS)*, 2025. https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now.

Béchard, Deni Ellis. "How Drone Swarms Work — from Iran's Shahed Attack to Ukraine's Operation Spiderweb." *Scientific American*, June 16, 2025. https://www.scientificamerican.com/article/how-drone-swarms-work-from-irans-shahed-attack-to-ukraines-operation.

Dickinson, Peter. "Abkhazia Claims Shootdown of 2 Georgian Spy Drones." *Voice of America (VOA News)*, October 27, 2009. https://www.voanews.com/a/a-13-2008-05-04-voa21-66646552/557338.html.

Easter, Reagan. "U.S. Forces in the Middle East: Under Attack and Defending Israel." *Foundation for Defense of Democracies (FDD)*, June 16, 2025. https://www.fdd.org/analysis/policy_briefs/2025/06/16/u-s-forces-in-the-middle-east-under-attack-and-defending-israel.

Eslami, Mohammad. "Iran's Drone Supply to Russia and Changing Dynamics of the Ukraine War." *Journal for Peace and Nuclear Disarmament* 5, no. 2 (November 20, 2022): 1–12. https://doi.org/10.1080/25751654.2022.2149077.

Espreso TV. "French Aeronaut Explains Why Russian Army Is Unable to Use Drones Effectively." *Espreso*, May 9, 2023. https://global.espreso.tv/french-aeronaut-explains-why-russian-army-is-unable-to-use-drones-effectively.

European Commission. "Sanctions Adopted Following Russia's Military Aggression against Ukraine." *finance.ec.europa.eu*, 2023. https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en.

Franke, Ulrike. "Drones in Ukraine and Beyond: Everything You Need to Know." *European Council on Foreign Relations*, August 11, 2023. https://ecfr.eu/article/drones-in-ukraine-and-beyond-everything-you-need-to-know.

Franke, Ulrike. "Drones in Ukraine: Four Lessons for the West." *European Council on Foreign Relations (ECFR)*, January 10, 2025. https://ecfr.eu/article/drones-in-ukraine-four-lessons-for-the-west.

Hamadi, Ghadir. "What You Need to Know about the $2 Million Israeli Drone Hezbollah Shot down Yesterday." *L'Orient Today*, February 26, 2024. https://today.lorientlejour.com/article/1369444/what-you-need-to-know-about-the-2-million-israeli-drone-hezbollah-shot-down-today.html.

Gettinger, Dan. "'Drones Are Not Toys': The Russian Program." *Bard College Center for the Study of the Drone*, March 5, 2014. https://dronecenter.bard.edu/drones-toys-russian.

Guitton, Matthieu J. "Fighting the Locusts: Implementing Military Countermeasures against Drones and Drone Swarms." *Scandinavian Journal of Military Studies* 4, no. 1 (2021): 30–33. https://doi.org/10.31374/sjms.53.

Hijazi, Alaa, Christopher J. Ferguson, F. Richard Ferraro, Harold Hall, Mark Hovee, and Sherrie Wilcox. "Psychological Dimensions of Drone Warfare." *Current Psychology* 38, no. 5 (September 14, 2017): 1285–96. https://doi.org/10.1007/s12144-017-9684-7.

Hlotov, V., A. Hunina, S. Kniaziev, V. Kolesnichenko, and O. Prokhorchuk. "Analysis of Application of the UAVs for Military Tasks." *Modern Achievements of Geodesic Science and Industry* I, no. 37 (2019): 69–77. https://doi.org/10.33841/1819-1339-2019-1-37-69-77.

Holz, Jacob. "Victimhood and Trauma within Drone Warfare." *Critical Military Studies* 9, no. 2 (July 29, 2021): 1–16. https://doi.org/10.1080/23337486.2021.1953738.

Jeangène Vilmer, Jean-Baptiste. "Not so Remote Drone Warfare." *International Politics* 60 (July 22, 2021): 898. https://doi.org/10.1057/s41311-021-00338-9.

Jeffery, Capt., Van Bourgondien, David Matthews, and Raymond Franck. "Analysis of the Sustainment Organization and Process for the Marine Corps' RQ-11B Raven Small Unmanned Aircraft System (SUAS)." Naval Postgraduate School, 2012. https://www.dair.nps.edu/bitstream/123456789/2031/1/NPS-LM-12-010.pdf.

Jensen, Benjamin, and Yasir Atalan. "Drone Saturation: Russia's Shahed Campaign." *CSIS Briefs*, May 2025. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2025-05/250513_Jensen_Drone_Saturations.pdf.

Jensen, Benjamin. "Ukraine's Operation Spider-Web Upended Traditional Rules of War." *American University*, June 5, 2025. https://www.american.edu/sis/news/20250605-ukraines-operation-spider-web-upended-traditional-rules-of-war.cfm.

Kofman, Michael. "Russian Performance in the Russo-Georgian War Revisited." *War on the Rocks*, September 4, 2018. https://warontherocks.com/2018/09/russian-performance-in-the-russo-georgian-war-revisited.

Library of Congress. "Research Guides: BRICS: Sources of Information: Introduction." *Library of Congress*, 2016. https://guides.loc.gov/brics.

Luzin, Pavel. "Russian Military Drones: Past, Present, and Future of the UAV Industry." *Foreign Policy Research Institute*, November 2023. https://www.fpri.org/wp-content/uploads/2023/11/russian-military-drones-.pdf.

Maj, Philip. *The Soviet Air Force and Strategic Bombing: A Research Report Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements.*

Advisor Major Thomas Meara. Maxwell Air Force Base: Air University, 1999. https://apps.dtic.mil/sti/tr/pdf/ADA398859.pdf.

Mahadevan. "The Military Utility of Drones." *ETH Zurich* no. 78 (July 2010): 2–4. https://doi.org/10.3929/ethz-a-006253833.

McDermott, Roger. "Russia's UAVs and UCAVs: ISR and Future Strike Capabilities." *The Jamestown Foundation*, March 23, 2022. https://jamestown.org/program/russias-uavs-and-ucavs-isr-and-future-strike-capabilities.

Military Factory. "HESA Qasef-1 Loitering Munition / UCAV Drone." *MilitaryFactory.com*, June 22, 2022. https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=2155.

Military Factory. "HESA Shahed-129 (Eye-Witness) Medium-Altitude, Long-Endurance (MALE) Reconnaissance / Light Attack Drone." *MilitaryFactory.com*, July 13, 2022. https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=1330.

Razooqi, Othman Dhari, and Alaa H. Ali. "Drones Neutralized by Utilize Electromagnetic Pulse (EMP) System." In *2022 5th International Conference on Engineering Technology and Its Applications (IICETA)*, no. 1 (May 31, 2022): 487–90. https://doi.org/10.1109/iiceta54559.2022.9888673.

On Demand News. "Intense Combat Footage Shows Mercenaries Fighting in Ukraine-Russia War | Full Series." *YouTube*, April 12, 2025. https://www.youtube.com/watch?v=pclT0pngf_k.

Patrick, Stewart, Erica Hogan, and Oliver Stuenkel. "BRICS Expansion and the Future of World Order: Perspectives from Member States, Partners, and Aspirants." *Carnegie Endowment for International Peace*, March 31, 2025. https://carnegieendowment.org/research/2025/03/brics-expansion-and-the-future-of-world-order-perspectives-from-member-states-partners-and-aspirants?lang=en.

Samus, Mykhailo. "Lessons Learned from the War in Ukraine: The Impact of Drones." *New Strategy Center*, 2024. https://newstrategycenter.ro/wp-content/uploads/2024/02/Lessons-Learned-from-the-War-in-Ukraine.-The-impact-of-Drones-2.pdf.

"Sukhoi Su-24 — Archived 3/2003." *Forecast International*. Accessed July 3, 2025. https://www.forecastinternational.com/archive/disp_old_pdf.cfm?ARC_ID=1047.

The Insider. "Four Rotors and a Prayer: How Russia Built a Billion-Ruble Drone Industry Using Chinese Parts." *The Insider*, May 16, 2025. https://theins.ru/en/inv/281354.

U.S. Air Force. “MQ-9 Reaper.” *U.S. Air Force*, September 23, 2015. https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper.

U.S. Army. “ODIN — OE Data Integration Network.” *ODIN (Operational Environment Data Integration Network)*. Accessed July 30, 2025. https://odin.tradoc.army.mil/Search/WEG/pchela.

U.S. Army. “ODIN — OE Data Integration Network.” *ODIN (Operational Environment Data Integration Network)*, 2025. https://odin.tradoc.army.mil/WEG/Asset/64d41728a7da9861432867e4a4fcef05.

3

Tech Diplomacy in the Age of AI: Power, Sovereignty, and the New Global Order

Hamza AARAB

Abstract: This chapter explores how artificial intelligence (AI) is redrawing the global balance of power, not through battlefield dominance but through data control, infrastructure dependency, and algorithmic influence. It analyzes how the United States, China, and the European Union each pursue distinct AI strategies and how tech diplomacy is emerging to mediate conflicts shaped by cloud reliance, compute inequality, and divergent regulatory visions. This paper argues that AI has become a core terrain of sovereignty and a catalyst for diplomatic realignment.

Keywords: Artificial Intelligence, Digital Sovereignty, Tech Diplomacy, Global Governance, Geopolitics

Introduction

At the United Kingdom's first-ever AI Safety Summit in 2023, the figure who captured global attention was not a political leader or military official, but Elon Musk — a tech entrepreneur whose public engagement with artificial intelligence continues to shape both popular and policy-level debates. Standing beside executives from OpenAI, Google DeepMind, and Microsoft, Musk warned that "there is some chance, above zero, that AI

will kill us all."[414] He was not alone in sounding the alarm. Geoffrey Hinton, widely regarded as the "Godfather of AI," resigned from Google that same year, warning that unregulated AI development could destabilize societies and endanger humanity.[415] Today, algorithms do not just sort information. They guide missiles, manage logistics, and monitor populations.

These concerns reflect a broader shift: the loudest voices influencing the trajectory of AI often emerge not from government ministries but from corporate boardrooms. Today's algorithms do more than sort data — they optimize military systems, manage logistics chains, and surveil populations.[416] Data centers now lie at the intersection of economic rivalry and national security. AI has become both a tool of statecraft and a contest for technological sovereignty.[417]

States no longer simply regulate AI; they are compelled to negotiate it. The architecture of digital power — servers, chips, cloud networks — is largely corporate, yet profoundly geopolitical. Who governs AI when its architects are private firms? Can a state claim sovereignty if its critical infrastructure is leased from abroad? And what happens when diplomacy must evolve faster than machine learning itself?

This is not speculative fiction; North Atlantic Treaty Organization (NATO) has launched AI hubs to anticipate future conflicts[418], and Defense Advanced Research Projects Agency (DARPA) funds autonomous defense systems.[419] China and the United States (U.S.) clash over semiconductor dominance, with companies like NVIDIA and Huawei at the heart of a new strategic race.[420]

---

[414] *"AI One of the Biggest Threats to Humanity: Elon Musk," Free Press Journal*, 2023.

[415] Analisa Novak, "'Godfather of AI' Geoffrey Hinton Warns AI Could Take Control from Humans," *CBS News*, 2025.

[416] *Artificial Intelligence in Aerospace & Defense — Global Strategic Business Report* (Research and Markets, 2025).

[417] Daniel Mügge, "EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?" *Journal of European Public Policy*, 2024.

[418] *NATO DIANA*, n.d., https://www.diana.nato.int.

[419] *David Vergun, "DARPA Aims to Develop AI, Autonomy Applications Warfighters Can Trust," U.S. Department of Defense, 2024.*

[420] FP Analytic, "Semiconductors and the U.S.-China Innovation Race," *Foreign Policy*, 2021.

Meanwhile, the European Union (EU) advances its AI Act, aiming not to control infrastructure but to lead in setting global rules.[421]

This paper does not offer a warning about dystopia, nor does it celebrate unchecked innovation. It examines how artificial intelligence is reshaping global diplomacy, redefining sovereignty, and redrawing the boundaries of international governance. By the end of this chapter, we will have mapped how states, corporations, and institutions are negotiating a new geopolitical grammar — written not in treaties, but in training data, compute capacity, and algorithmic power.

AI as a Geopolitical Force

In 2025, AI steers choices via invisible systems. As Nicholas Wright observed about China, "It is not like you are exporting communism. You are exporting a system of control."[422] In today's world, power is asserted not by flags but by software, standards, and surveillance. Policymakers are responding by proposing model registries and watermarking systems to authenticate AI outputs — an effort to engineer trust in an era where influence flows through code.[423] The new contest is not about who builds the smartest AI but rather who sets the rules it operates by. Sovereignty now hinges on who defines digital norms, controls platforms, and governs systems.

Military strategy is shifting from troops to tech: AI powers logistics, drones, and predictive surveillance. The U.S. invests through DARPA's "AI Next" program, while China embeds AI across its surveillance and cyber operations under a civil-military fusion model.[424] Intelligence is shifting from spies to sensors; governments now deploy algorithmic systems to

---

[421] European Union, *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 26 June 2024 on Artificial Intelligence*, *Official Journal of the European Union*, 2024.

[422] Steve LeVine, "Orwellian Surveillance Is Changing Us, and It's Powered by AI," *Axios*, 2018.

[423] National Telecommunications and Information Administration (NTIA), *AI Output Disclosures: Use, Provenance, Adverse Incidents*, 2024.

[424] Defense Advanced Research Projects Agency (DARPA), "AI Next," 2018; Elsa B. Kania, "AI Weapons in China's Military Innovation," *Brookings*, 2020.

monitor dissent, anticipate unrest, and shape public narratives in real time. However, as these systems grow more autonomous, debates have intensified around creating emergency protocols, such as "kill switches," to prevent runaway harm.[425] Meanwhile, alignment science has emerged as a critical research frontier, aiming to ensure that AI systems remain under meaningful human control, even in crisis conditions.[426] China's export of surveillance tools to over 60 countries reinforces what analysts call "techno-authoritarianism."[427] As Ian Hogarth has argued, the ability to develop and control advanced AI systems will shape global hierarchies and the flow of information, echoing the strategic weight of nuclear capabilities in the 20th century.[428]

Economic power now centers on controlling the AI supply chain. High-end AI requires compute capacity, chip clusters, hyperscale data centers, and submarine cables as the new arteries of global power. The U.S. launched the $500 billion "Stargate" initiative to secure domestic compute and counter China's scaling.[429] Strategic assets, such as Meta's Waterworth cable and Dubai's data centers, demonstrate how compute infrastructure has become modern-day sovereignty pipelines.[430] [431] This digital infrastructure scramble revives sovereignty questions as "compute governance"; controlling high-density compute clusters is now as vital to national security as 20th-century energy reserves.[432]

Soft power in the AI era is conveyed through the values embedded in algorithms. American firms promote openness and market-based innovation; China exports a model anchored in state control, centralized planning, and

---

[425] Alasdair Lane, "Beyond a Kill Switch: Safeguarding the Future of AI," *Politico*, 2025.

[426] SHEN et al., *Towards Bidirectional Human-AI Alignment: A Systematic Review for Clarifications, Framework, and Future Directions*, *ACM*, 2024.

[427] Maya Wang, "China's Techno-Authoritarianism Has Gone Global," *Human Rights Watch*, 2021.

[428] Ian Hogarth, "AI Nationalism," 2018.

[429] OpenAI, "Announcing the Stargate Project," 2025.

[430] Gaya Nagarajan and Alex-Handrah Aimé, "Unlocking Global AI Potential with Next-Generation Subsea Infrastructure," *Meta*, 2025.

[431] Elwely Elwelly, "Dubai's du Announces 2 Billion Dirhams Hyperscale Data Center Deal with Microsoft," *Reuters*, 2025.

[432] Sijarvis, *Compute Governance Literature Review*, *LessWrong*, 2024.

regulatory sovereignty. As Ivana Bartoletti notes, AI systems do not merely function; they encode political and cultural assumptions.[433] Chris Miller describes this as a "Code War," a new form of geopolitical rivalry waged through training data, model weights, and algorithmic values.[434]

These dynamics are not hypothetical. Major powers are embedding AI into their core strategies, reflecting competing visions of autonomy, control, and governance. What follows is a closer look at how the U.S., China, and the EU are navigating this emerging terrain:

United States

The U.S. leads the world in foundational AI research and development. Initiatives such as the National AI Initiative Act (2021) and consistent funding by agencies like DARPA reflect a strategy aimed at achieving technological supremacy through public-private innovation collaboration.[435] Major U.S. companies, including OpenAI, Microsoft, Google, and NVIDIA, dominate the global AI ecosystem, particularly in large language models, cloud infrastructure, and semiconductors. However, the American approach to AI governance remains fragmented. Unlike China or the EU, the U.S. lacks a binding AI law. This reflects an embedded belief in market-led governance, where innovation is prioritized over-regulation.[436] This model empowers Big Tech companies *(i.e., dominant technology firms such as Google, Apple, Meta, Microsoft, and Amazon, which exert disproportionate control over digital markets, infrastructure, and data ecosystems)* to act as informal diplomatic actors. Microsoft, for example, has promoted its Cloud for Sovereignty program as a solution for nations seeking digital autonomy.[437] Meanwhile, OpenAI CEO Sam Altman has actively engaged

---

[433] Ivana Bartoletti, *An Artificial Revolution: On Power, Politics and AI*, *AI Policy Exchange*, 2020.

[434] Chris Miller, "Chip War: The Fight for the World's Most Critical Technology," *Geopolitica.info*, 2022.

[435] U.S. Congress, *H.R.6216 — National Artificial Intelligence Initiative Act of 2020*, 2020.

[436] Benjamin Cedric Larsen and Sabrina Küspert, "Regulating General-Purpose AI: Areas of Convergence and Divergence Across the EU and the US," *Brookings*, 2024.

[437] Corey Sanders, "Microsoft Cloud for Sovereignty: The Most Flexible and Comprehensive Solution for Digital Sovereignty," *Microsoft*, 2022.

in international forums and testified before the U.S. Congress, advocating for a U.S.-led global AI alliance.[438] Nevertheless, critics argue that this convergence of corporate and state power risks allowing private interests to dictate the shape of global governance.[439]

China

China treats artificial intelligence not merely as a tool of modernization but as a pillar of national power. Its 2017 AI Development Plan set a goal of global leadership by 2030. The strategy is state-driven, leveraging public funding, embedding AI goals within its Five-Year Plans, and aligning development with national security priorities.[440] Firms like Baidu, Alibaba, and Tencent operate under a civil-military fusion model extending AI into surveillance, cyber-intelligence, and governance. AI is embedded not only in commercial products but also in state apparatuses, including smart cities, facial recognition, and social credit systems.[441] Tools developed under this model have been exported to dozens of countries through the Digital Silk Road *(i.e., China's global initiative to export digital infrastructure and tech standards via the Belt and Road framework)*, extending China's vision of techno-sovereignty.[442] However, resistance is growing. Nations are revisiting deals, and U.S.-led chip controls have slowed China's access to AI hardware. Nevertheless, China's vertically integrated approach to AI governance remains appealing to states seeking technological advancement without liberal political constraints.[22]

---

[438] Chris McKay, "Sam Altman Advocates for U.S. Leadership in AI Development," *Maginative*, 2024.

[439] Harvard Law Review Association, "Co-Governance and the Future of AI Regulation," *Harvard Law Review* 138 (2025): 1609.

[440] Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," *Stanford University*, 2017.

[441] Elsa B. Kania, *Testimony Before the U.S.-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion*, *Center for a New American Security*, 2019.

[442] Bulelani Jili, "China's Surveillance Ecosystem and the Global Spread of Its Tools," *Atlantic Council*, 2022.

European Union

The EU has taken a distinct approach, governing through norms rather than military or economic dominance. The General Data Protection Regulation (GDPR) and the 2024 AI Act position the EU as a global leader in ethical, human-centric AI regulation.[443] Europe's model centers on the concept of digital sovereignty, emphasizing the ability to govern digital infrastructure, data flows, and algorithmic systems independently. Leaders like the French president Macron frame this as key to preserving democratic agency.[444] To that end, the EU has invested in initiatives such as GAIA-X (a sovereign European cloud infrastructure), supported open-source AI development, and imposed mandatory transparency standards on opaque black-box models.[445] However, Europe's regulatory strength is not matched by industrial capacity, a paradox at the heart of its digital strategy. The absence of AI giants comparable to those in the U.S. or China raises questions about the EU's ability to enforce its standards effectively.[446] Still, the so-called "Brussels Effect" ensures that European rules often shape global markets, either through direct adoption or by setting *de facto* international norms.[447]

Beyond national strategies, a new form of power projection is emerging: the ability to enforce global AI standards through voluntary treaties, bilateral tech pacts, and supranational initiatives, such as model registries and safety laboratories. These cases reveal a truth: AI governance plays out on ideologically charged terrain. Beyond these national strategies lies a deeper transformation, one that recasts power not through territorial expansion but through control over data flows, technical standards, and digital infrastructure. The new contest is over who shapes the invisible architectures

---

[443] European Parliament and Council of the European Union, *Regulation (EU) 2016/679 — General Data Protection Regulation*, *Official Journal of the European Union*, 2016.

[444] Camille Bello, "VivaTech 2023: Emmanuel Macron Unveils Ambitious Plan to Boost French AI and Tech Start-Ups," *Euronews*, 2023.

[445] Francesco Bonfiglio, *Vision & Strategy*, *Gaia-X*, 2021.

[446] Raluca Csernatoni, "The EU's AI Power Play: Between Deregulation and Innovation," *Carnegie Institute*, 2025.

[447] Charlotte Siegmann and Markus Anderljung, *The Brussels Effect and Artificial Intelligence*, *Centre for the Governance of AI*, 2022.

of modern life. Sovereignty is shifting from soil to servers, and this shift is already redrawing the global map, not on paper, but in code.

Digital Sovereignty in the AI Era

In the algorithmic age, sovereignty extends beyond borders to backend control. Digital sovereignty refers to a state or region's ability to govern its infrastructure, data flows, and algorithmic systems independently, without external interference.[448] As AI embeds itself in defense, healthcare, finance, and elections, the ability to control these systems becomes a new marker of autonomy. This shift is not theoretical; the U.S. CLOUD Act grants extraterritorial access to data stored by American firms abroad,[449] prompting European calls for "strategic autonomy" through initiatives like the AI Act and GAIA-X. Different regions reflect their political DNA in how they pursue digital sovereignty. China's "cyber-sovereignty" model mandates data localization, surveillance infrastructure, and alignment with security priorities.[450] The EU, in contrast, promotes ethical governance and democratic resilience.[451] Developing countries remain on the periphery, lacking infrastructure, talent, and access to foundational AI tools. Researchers warn that this creates a technological divide and reinforces digital dependencies, echoing colonial patterns.[452] In response, the Global South is pushing back. The African Union's (AU) Digital Transformation Strategy and South-South AI collaborations aim to develop independent cloud infrastructures, AI research hubs and shared compute platforms.[453]

---

[448] Gábor Hulkó, Janos Kalman, János Kálmán, and András Lapsánszky, "The Politics of Digital Sovereignty and the European Union's Legislation: Navigating Crises," *Frontiers*, 2025.

[449] Peter Church and Caitlin Potratz Metcalf, "U.S. CLOUD Act and GDPR — Is the Cloud Still Safe?" *Linklaters*, 2019.

[450] ARTICLE 19, *Cybersecurity with Chinese Characteristics: Digital Governance in the Indo-Pacific and the Taiwanese Alternative*, *Columbia Global Freedom of Expression*, 2025.

[451] Isabelle Yr Carlsson and Milan Strahm, "EU a 'Reliable Partner' for Digital Cooperation Amid Turbulence, Tech Chief Says," *Reuters*, 2025.

[452] Vili Lehdonvirta, Boxi Wu, and Zoe Hawkins, "Compute North vs. Compute South: The Uneven Possibilities of Compute-Based AI Governance Around the Globe," *SocArXiv Preprint*, 2024.

[453] African Union, *The Digital Transformation Strategy for Africa (2020–2030)*, 2020.

These initiatives are not just technical responses but political statements and assertions that future AI ecosystems must not simply replicate colonial dependencies under digital guises.

Sovereignty is no longer protected with tanks or tariffs but with chips, clouds, and code. Moreover, as dependency on foreign tech erodes autonomy, many countries are rewriting their digital playbooks. One of the most prominent moves is data localization. Russia and China have long mandated that sensitive data remain within their borders under the banner of national security, and India has followed suit in sectors such as finance and health.[454] The EU's GDPR stops short of mandating localization but effectively pressures firms to host data regionally.[31] Beyond data, the semiconductor supply chain has become the frontline of sovereignty. The global chip shortage, compounded by U.S. export bans on advanced semiconductors to China, highlighted the fragility of existing dependencies.[455] In response, the EU launched its €43 billion Chips Act, the U.S. passed the CHIPS and Science Act, and China accelerated its indigenous ecosystem through SMIC and Baidu's Kunlun chips.[456]

However, sovereignty now means more than owning hardware; it means governing the compute that trains frontier AI. This is the new battleground. Nations are racing not only to secure chip fabrication but also to establish sovereign access to high-performance computing clusters and cloud networks capable of training large-scale AI systems. This race risks deepening the global digital divide. At the same time, nations are asserting control over the algorithmic layer. The EU, UK, and others have launched Model Registries and Safety Labs to verify, register, and stress-test high-risk AI before deployment.[457] These registries represent a quiet revolution

---

[454] Nigel Cory and Luke Dascoli, "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them," *Information Technology & Innovation Foundation*, 2021.

[455] Sujai Shivakumar, Charles Wessner, and Thomas Howell, "Balancing the Ledger: Export Controls on U.S. Chip Technology to China," *CSIS*, 2024.

[456] European Commission, *European Chips Act*, 2023; U.S. Congress, *H.R.4346 — CHIPS and Science Act*, *Congress.gov*, 2021*;* Reuters, "Baidu Says 2nd-Gen Kunlun AI Chips Enter Mass Production," 2021.

[457] Department for Science, Innovation & Technology, *Emerging Processes for Frontier AI Safety*, *GOV.UK*, 2023.

in governance, where the right to innovate increasingly comes with obligations to disclose, document, and demonstrate safety at scale. Diplomatically, the sovereignty race is producing a patchwork of bilateral tech pacts. The U.S.–UK Declaration on AI Safety, the EU–Japan Digital Partnership, and similar agreements mark a shift toward ad-hoc alliances aimed at sharing computing resources, setting joint standards, and securing trusted supply chains outside formal global institutions,[458] which reflects a world where tech sovereignty increasingly plays out through fragmented but strategic alignments.

The global race for digital sovereignty has accelerated, but it is far from a level playing field. A growing concern is the emergence of "compute deserts," regions that lack access to high-performance computing (HPC) infrastructure necessary for training or deploying cutting-edge AI models.[40] As Large Language Models (LLMs) *(i.e., AI systems trained on massive text datasets to generate human-like language)* demand exponentially more compute, the gap between infrastructure-rich and -poor nations widens, risking hard-coded digital inequality. Without equitable access to semiconductors, cloud capacity, and skilled labor, entire regions risk being relegated to the margins of AI development. The problem is compounded by deep interdependence: AI runs on global datasets, Taiwan-made chips, and U.S.-controlled clouds, and even tech powers like China and the U.S., despite efforts at self-reliance, remain entangled in global supply chains. These dependencies expose the limits of full sovereignty and challenge techno-nationalist ambitions.

Meanwhile, policy fragmentation is undermining the pursuit of coherent global governance. The U.S. leans into private-sector innovation with limited regulation, China doubles down on centralized control, and the EU advances a rights-based model through its AI Act. This AI balkanization results in regulatory collisions, complicating international cooperation on pressing issues such as disinformation, AI ethics, and autonomous weapons.[459]

---

[458] Will Henshall, "U.S., U.K. Announce Partnership to Safety Test AI Models," *Time*, 2024; European Council, "EU and Japan Reinforce Tech and Digital Partnership," 2025.

[459] H. Akin Ünver, *Artificial Intelligence (AI) and Human Rights: Using AI as a Weapon of Repression and Its Impact on Human Rights*, *European Parliament*, 2024.

In response to these risks, some governments have begun discussing the integration of "emergency kill switches," now being explored as a last-resort mechanism to shut down dangerously misaligned AI systems. While these proposals are controversial, they underscore the profound intersection of digital sovereignty with national security imperatives.[13] Paradoxically, the sovereignty push can also backfire because, in regimes where democratic norms are weak, digital sovereignty may become a pretext for surveillance, censorship, and repression. States citing data independence and national security may, in fact, compromise civil liberties and silence dissent.[460] Thus, the challenge is dual: to reclaim digital agency without sacrificing openness and to design sovereignty frameworks that protect both autonomy and rights. In short, the quest for digital sovereignty is not just about cables, chips, and clouds; it is about values, geopolitics, and power. It calls for more than national policy alone: it requires visionary diplomacy, ethical foresight, and inclusive international dialogue on how technology should serve humanity. As power shifts from parliaments to platforms and from ministries to machine-learning labs, diplomacy must evolve to meet the moment. The next frontier lies not only in governing technology but in redefining the very institutions through which that governance is negotiated.

Tech Diplomacy and Global Governance

In 2025, Sam Altman of OpenAI joined world leaders at the Paris AI Action Summit, not as a tech CEO, but as a diplomatic voice, pushing for interoperable AI safety norms in a scene that was unthinkable a decade ago.[461] Welcome to tech diplomacy: a new arena where states, tech giants like Google and Huawei, and Non-governmental organizations (NGOs) like The Future Society shape the global AI landscape. Unlike traditional diplomacy, which relies on treaties and visible borders, tech diplomacy navigates a borderless domain of code, compute, and cloud infrastructures. It addresses the

[460] Adrian Shahbaz, *The Rise of Digital Authoritarianism*, *Freedom House*, 2018.

[461] Pascale Davies, "Paris AI Action Summit: From DeepSeek to Europe's Path, Here's Everything You Need to Know," *Euronews*, 2025.

shifting terrain of global power through three main functions: setting ethical standards, building trust amid cyber threats, and expanding capacity for the Global South.[462] Nevertheless, as 2025 U.S. tariffs fracture tech supply chains and EU leaders push for digital sovereignty, the paradox deepens: how can diplomacy bridge a world divided by competing digital ambitions? This transformation goes beyond new players and platforms. It marks a redefinition of sovereignty itself. Where territorial borders once signified power, today it is server farms, model registries, and cloud ecosystems that determine strategic influence. Strategic influence now depends on controlling the infrastructures that train, deploy, and secure artificial intelligence. These invisible architectures evolve more rapidly than traditional diplomatic frameworks can adapt, exposing the limitations of state-centered, treaty-driven governance. In this context, tech diplomacy emerges not simply as a response to technological change, but as the necessary mechanism to govern the new foundations of global order.

First, tech diplomacy plays a norm-setting role, establishing common ethical frameworks and technical standards for the development of AI. The Organisation for Economic Co-operation and Development (OECD) AI Principles, endorsed by over 40 countries in 2019, mark one of the earliest multilateral efforts to define trustworthy AI. These guidelines were shaped not only by governments but also by civil society and firms like Google, IBM, and Microsoft, and their internal ethics charters helped influence broader global discourse.[463] Similarly, the Global Partnership on AI (GPAI) represents a hybrid model of state and non-state participation in developing global frameworks for safety, fairness, and transparency.[464] These tools aim to catch risks early through model registration, stress-testing for systemic vulnerabilities, and traceability mechanisms to combat disinformation in sectors like elections and media.

---

[462] Mouloud Khelif, "Tech Diplomacy: Unlocking Solutions to Global Challenges in a Tech-Driven World," *Geneva Graduate Institute*, 2023*; Mouloud Khelif, "Tech Diplomacy Could Help Solve Global Challenges," Diplo Foundation, 2023.*

[463] Lucia Russo and Noah Oder, "How Countries Are Implementing the OECD Principles for Trustworthy AI," *OECD*, 2023.

[464] OECD, *Global Partnership on Artificial Intelligence*, 2024.

Second, tech diplomacy plays a role in trust-building and conflict prevention. In a world of algorithmic opacity, predictive surveillance, and AI-enhanced cyber weapons, trust is both fragile and critical.[465] Tech diplomacy promotes transparency through disclosure obligations, shared safety protocols, and cross-border data dialogue. The UN Office for Disarmament Affairs has convened discussions on lethal autonomous weapons systems (LAWS), where governments and private actors debate ethical boundaries.[466] Similarly, initiatives like the AI Safety Summit in Bletchley Park in 2023 brought together governments and tech leaders to address existential risks from frontier models and formulate minimum safety standards, thereby blurring traditional diplomatic boundaries.[467] Alignment science, as mentioned before, has also entered diplomatic discourse, with researchers collaborating across borders on interpretability, robustness, and oversight techniques. These technical guardrails are no longer academic projects; they are becoming instruments of national security policy.

Third, tech diplomacy engages in capacity building, particularly for countries excluded from the high-tech core. Initiatives such as the International Telecommunication Union (ITU)'s AI for Good, UNESCO's AI ethics recommendations, and Google's support for African labs help expand digital infrastructure, ethical training, and policymaking capacity.[468] Without these efforts, much of the Global South risks becoming passive recipients rather than active shapers of the AI revolution. In parallel, Global South actors are launching their own governance initiatives, including the AU's Data Policy Framework, as well as Brazil and Indonesia's push for a Global Compute Compact.[469] These efforts aim to reduce dependency on Western

---

[465] Miles Brundage et al., *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, *Cornell University*, 2018.

[466] UNODA, *Lethal Autonomous Weapon Systems (LAWS)*, 2023.

[467] United Kingdom, Prime Minister's Office, *AI Safety Summit 2023*, *GOV.UK*.

[468] ITU, *AI for Good*, 2017; UNESCO, *Recommendation on the Ethics of Artificial Intelligence*, 2023; Matt Brittin, "Africa's Digital Decade: AI Upskilling and Expanding Speech Technology," *Google*, 2024.

[469] Africa Union, *AU Data Policy Framework*, 2022; Obinna Isiadinso, "Brazil's $350B Data Center Power Play: Why the Future of AI Infrastructure May Skip the U.S.," *Global Data Center Hub*, 2025; Tuhu Nugraha, "Leveraging the BRICS Network to Drive Indonesia's AI Strategy," *Modern Diplomacy*, 2024.

infrastructures and advocate for equitable access to training resources, model weights, and data sovereignty.

Together, these dynamics signal a shift from law-based governance to values-driven coordination, where norms evolve through dialogue, pilot programs, and voluntary mechanisms, not top-down regulation. Unlike the governance of nuclear weapons or global finance, AI governance is unfolding as a polycentric arena, where influence is distributed, and legitimacy flows from collaboration rather than coercion. Here, tech diplomacy is less about advancing national interests and more about mediating between actors with unequal capabilities but shared risks. The challenge is profound: how to create trust in a world of proprietary algorithms and geopolitical rivalry and how to ensure that AI governance reflects not just the power of those who build it, but the values of those who must live with its consequences.

This normative shift, however, is not unfolding without friction. A striking example came in 2025 when U.S. tariffs on EU and Chinese tech exports triggered a digital backlash. These trade barriers, along with Washington's exclusion of tech services from EU negotiations, reflected a deliberate strategy to shield U.S. AI monopolies from European regulation.[470] The EU, in turn, has doubled down on digital sovereignty, with leaders at the Paris Peace Forum 2025 calling for local AI ecosystems to reduce their reliance on U.S. cloud and compute platforms.[471] The clash exposed a deeper divide: the EU aims to discipline AI through legal frameworks, while the U.S. defends its digital edge through policy hardball. Far from abstract, this conflict complicates efforts to harmonize AI governance and reveals just how intertwined tech diplomacy has become with strategic protectionism.

To stay relevant in the algorithmic age, tech diplomacy must shift from summits to substance. As the UN's Governing AI for Humanity report (2024) notes, this evolution demands more than consensus-building;

[470] Dtalliance, *DigiTrade Digest*, no. 135, 2025.

[471] Supantha Mukherjee, "Nvidia's Pitch for Sovereign AI Resonates with EU Leaders," *Reuters*, 2025.

it requires concrete infrastructure for global equity in AI governance.[472] This means building sovereign compute capacity, funding multilingual and open-source models, and creating public-interest data ecosystems. Without such foundations, the governance of AI will remain skewed, shaped by those who control the infrastructures and design the learning systems. Efforts like the Tech Diplomacy Network, which embeds digital attachés in global tech hubs, reflect this emerging logic: representation in AI policymaking now requires digital fluency, not just diplomatic protocol.[473] Equally, tech diplomacy must become the vehicle for setting enforceable red lines, especially on frontier risks like lethal autonomous weapons or mass surveillance systems. The Bletchley Park AI Safety Summit in 2023 underscored this urgency, yet its voluntary outcomes highlight a deeper truth: principles without enforcement are politics without power.[61] New models must enable institutions, regional or global, to not only debate but implement AI norms. The AU's Digital Transformation Strategy offers a case in point. It reframes governance not as the adoption of global standards but as co-authorship of them.[41] Tech diplomacy, if it is to write the grammar of digital geopolitics, must now speak in clauses of accountability, equity, and enforceable cooperation, not just ambition.

Conclusion

The 2025 Paris AI Summit opened with the voices of tech CEOs, but it ends, symbolically, with a question echoing in every capital: Who governs the governors of AI? After journeying through the linked domains of algorithms, sovereignty, and diplomacy, one thing is clear: AI is not just reshaping geopolitics, it is becoming geopolitics. This paper has mapped a world in flux, where AI is not merely a tool of governance but a terrain of governance itself. Nations like the U.S., China, and those of the EU are not just racing to develop AI, they are racing to define what kind of world it should serve. Washington bets on innovation and global market

[472] UN AI Advisory Body, *Governing AI for Humanity: Final Report*, 2024.

[473] Tech-Diplomacy. *What Is Tech Diplomacy?* n.d. https://www.tech-diplomacy.org.

leadership; Beijing invests in infrastructural diplomacy and centralized digital governance; Brussels carves a path through ethical regulation and digital rights. However, amidst this competition, another dynamic unfolds: tech diplomacy, where embassies meet data centers, and negotiations happen between diplomats and developers. Private firms, from OpenAI to Huawei, no longer only lobby for policy; instead, they shape it. The result is a fractured governance landscape: promising but unequal, collaborative but cautious. Still, the future is not sealed. There remains a narrow, urgent space for cooperative frameworks, pluralistic dialogue, and inclusive diplomacy. Cities like Geneva are already hosting new diplomatic forums on AI and digital rights. Nations from the Global South are demanding equity in compute access, standard-setting, and data governance. Moreover, young technologists are reframing sovereignty not just as control but as consent.

So, where does that leave us? It leaves us at the threshold of a new diplomatic age, one where cables and code shape borders as much as treaties and tanks. Where governing AI means governing the very architecture of decision-making in war, peace, and daily life. And where the most important negotiations are no longer just about land or oil but about data, ethics, and control over the invisible hands that shape our world. Ultimately, the future of AI governance is not solely about who writes the rules. It is about who gets to imagine them in the first place.

Bibliography

African Union. *AU Data Policy Framework*. 2022. https://au.int/en/documents/20220728/au-data-policy-framework.

African Union. *The Digital Transformation Strategy for Africa (2020–2030)*. 2020. https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

ARTICLE 19. *Cybersecurity with Chinese Characteristics: Digital Governance in the Indo-Pacific and the Taiwanese Alternative*. Columbia Global Freedom of Expression, 2025. https://globalfreedomofexpression.columbia.edu/publications/cybersecurity-with-chinese-characteristics-digital-governance-in-the-indo-pacific-and-the-taiwanese-alternative.

Bello, Camille. "VivaTech 2023: Emmanuel Macron Unveils Ambitious Plan to Boost French AI and Tech Start-Ups." *Euronews*, 2023. https://www.euronews.com/next/2023/06/14/macron-unveils-ambitious-plan-to-boost-french-ai-and-tech-start-ups-at-vivatech.

Bartoletti, Ivana. *An Artificial Revolution: On Power, Politics and AI*. AI Policy Exchange, 2020. https://aipolicyexchange.org/2020/05/20/an-artificial-revolution-on-power-politics-and-ai.

Bonfiglio, Francesco. *Vision & Strategy*. Gaia-X, 2021. https://gaia-x.eu/wp-content/uploads/2021/12/Vision-Strategy.pdf.

Brittin, Matt. "Africa's Digital Decade: AI Upskilling and Expanding Speech Technology." *Google*, 2024. https://blog.google/around-the-globe/google-africa/africas-digital-decade.

Brundage, Miles, et al. *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Cornell University, 2018. https://arxiv.org/abs/1802.07228.

Carlsson, Isabelle Yr, and Milan Strahm. "EU a 'Reliable Partner' for Digital Cooperation Amid Turbulence, Tech Chief Says." *Reuters*, 2025. https://www.reuters.com/sustainability/boards-policy-regulation/eu-reliable-partner-digital-cooperation-amid-turbulence-tech-chief-says-2025-06-05.

Church, Peter, and Caitlin Potratz Metcalf. "U.S. CLOUD Act and GDPR – Is the Cloud Still Safe?" *Linklaters*, 2019. https://www.linklaters.com/en/insights/blogs/digilinks/2019/september/us-cloud-act-and-gdpr-is-the-cloud-still-safe.

Cory, Nigel, and Luke Dascoli. "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them." *Information Technology & Innovation Foundation*, 2021. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost.

Csernatoni, Raluca. "The EU's AI Power Play: Between Deregulation and Innovation." *Carnegie Institute*, 2025. https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation?lang=en.

Davies, Pascale. "Paris AI Action Summit: From DeepSeek to Europe's Path, Here's Everything You Need to Know." *Euronews*, 2025. https://www.euronews.com/next/2025/02/10/paris-ai-summit-from-deepseek-to-europes-path-heres-everything-you-need-to-know.

Defense Advanced Research Projects Agency (DARPA). "AI Next." 2018. https://www.darpa.mil/research/programs/ai-next.

Department for Science, Innovation & Technology. *Emerging Processes for Frontier AI Safety*. GOV.UK, 2023. https://www.gov.uk/government/publications/emerging-processes-for-frontier-ai-safety/emerging-processes-for-frontier-ai-safety.

Dtalliance. *DigiTrade Digest #135*. 2025. https://dtalliance.org/2025/04/15/digitrade-digest-135.

Elwelly, Elwely. "Dubai's du Announces 2 Billion Dirhams Hyperscale Data Center Deal with Microsoft." *Reuters*, 2025. https://www.reuters.com/business/media-telecom/dubais-du-announces-2-billion-dirhams-hyperscale-data-center-deal-with-microsoft-2025-04-22.

European Commission. *European Chips Act*. 2023. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en.

European Council. "EU and Japan Reinforce Tech and Digital Partnership." 2025. https://digital-strategy.ec.europa.eu/en/news/eu-and-japan-reinforce-tech-and-digital-partnership.

European Parliament and Council of the European Union. *Regulation (EU) 2016/679 — General Data Protection Regulation*. *Official Journal of the European Union*, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

European Union. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 26 June 2024 on Artificial Intelligence*. *Official Journal of the European Union*, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689.

FP Analytic. "Semiconductors and the U.S.-China Innovation Race." *Foreign Policy*, 2021. https://foreignpolicy.com/2021/02/16/semiconductors-us-china-taiwan-technology-innovation-competition.

Free Press Journal. "AI One of the Biggest Threats to Humanity: Elon Musk." 2023. https://www.freepressjournal.in/world/ai-one-of-the-biggest-threats-to-humanity-elon-musk.

Harvard Law Review Association. "Co-Governance and the Future of AI Regulation." *Harvard Law Review* 138 (2025): 1609. https://harvardlawreview.org/print/vol-138/co-governance-and-the-future-of-ai-regulation.

Henshall, Will. "U.S., U.K. Announce Partnership to Safety Test AI Models." *Time*, 2024. https://time.com/6962503/ai-artificial-intelligence-uk-us-safety.

Hogarth, Ian. "AI Nationalism." *Personal Blog*, 2018. https://www.ianhogarth.com/blog/2018/6/13/ai-nationalism.

Hulkó, Gábor, Janos Kalman, János Kálmán, and András Lapsánszky. "The Politics of Digital Sovereignty and the European Union's Legislation: Navigating Crises."

Frontiers in Political Science, 2025. https://www.frontiersin.org/journals/political-science/articles/10.3389/fpos.2025.1548562/full.

International Telecommunication Union (ITU). *AI for Good*. 2017. https://aiforgood.itu.int.

Isiadinso, Obinna. "Brazil's $350B Data Center Power Play: Why the Future of AI Infrastructure May Skip the U.S." *Global Data Center Hub*, 2025. https://www.globaldatacenterhub.com/p/brazils-350b-data-center-power-play.

Jili, Bulelani. "China's Surveillance Ecosystem and the Global Spread of Its Tools." *Atlantic Council*, 2022. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools. https://www.politico.com/sponsored/2025/02/beyond-a-kill-switch-safeguarding-the-future-of-ai.

Kania, Elsa B., Graham Webster, Rogier Creemers, and Paul Triolo. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)." *Stanford University DigiChina*, 2017. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017.

Kania, Elsa B. *Testimony before the U.S.-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion*. Center for a New American Security, 2019.

Kania, Elsa B. "AI Weapons in China's Military Innovation." *Brookings*, 2020. https://www.brookings.edu/articles/ai-weapons-in-chinas-military-innovation. https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence.pdf.

Khelif, Mouloud. "Tech Diplomacy: Unlocking Solutions to Global Challenges in a Tech-Driven World." *Geneva Graduate Institute*, 2023. https://executiveeducation.blog/themes/digital/tech-diplomacy-unlocking-solutions-to-global-challenges-in-a-tech-driven-world.

Lane, Alasdair. "Beyond a Kill Switch: Safeguarding the Future of AI." *Politico*, 2025. Khelif, Mouloud. "Tech Diplomacy Could Help Solve Global Challenges." *Diplo Foundation*, 2023. https://www.diplomacy.edu/blog/tech-diplomacy-could-solve-global-challenges.

Larsen, Benjamin Cedric, and Sabrina Küspert. "Regulating General-Purpose AI: Areas of Convergence and Divergence Across the EU and the US." *Brookings*, 2024. https://www.brookings.edu/articles/regulating-general-purpose-ai-areas-of-convergence-and-divergence-across-the-eu-and-the-us.

Lehdonvirta, Vili, Boxi Wu, and Zoe Hawkins. "Compute North vs. Compute South: The Uneven Possibilities of Compute-Based AI Governance Around the Globe." *SocArXiv Preprint*, 2024. https://osf.io/preprints/socarxiv/8yp7z_v1.

LeVine, Steve. "Orwellian Surveillance Is Changing Us, and It's Powered by AI." *Axios*, 2018. https://www.axios.com/2018/07/18/ai-geopolitics-surveillance-nightmare.

McKay, Chris. "Sam Altman Advocates for U.S. Leadership in AI Development." *Maginative*, 2024. https://www.maginative.com/article/sam-altman-advocates-for-u-s-leadership-in-ai-development.

Miller, Chris. "Chip War: The Fight for the World's Most Critical Technology." *Geopolitica.info*, 2022. https://www.geopolitica.info/fight-microchips-technology.

Mügge, Daniel. "EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?" *Journal of European Public Policy*, 2024. https://www.tandfonline.com/doi/full/10.1080/13501763.2024.2318475.

Mukherjee, Supantha. "Nvidia's Pitch for Sovereign AI Resonates with EU Leaders." *Reuters*, 2025. https://www.reuters.com/business/media-telecom/nvidias-pitch-sovereign-ai-resonates-with-eu-leaders-2025-06-16.

Nagarajan, Gaya, and Alex-Handrah Aimé. "Unlocking Global AI Potential with Next-Generation Subsea Infrastructure." *Meta*, 2025. https://engineering.fb.com/2025/02/14/connectivity/project-waterworth-ai-subsea-infrastructure.

National Telecommunications and Information Administration (NTIA). *AI Output Disclosures: Use, Provenance, Adverse Incidents*. 2024. https://www.ntia.gov/issues/artificial-intelligence/ai-accountability-policy-report/developing-accountability-inputs-a-deeper-dive/information-flow/ai-output-disclosures.

NATO DIANA. *Homepage*. n.d. https://www.diana.nato.int.

Novak, Analisa. "'Godfather of AI' Geoffrey Hinton Warns AI Could Take Control from Humans." *CBS News*, 2025. https://www.cbsnews.com/news/godfather-of-ai-geoffrey-hinton-ai-warning.

Nugraha, Tuhu. "Leveraging the BRICS Network to Drive Indonesia's AI Strategy." *Modern Diplomacy*, 2024. https://moderndiplomacy.eu/2024/12/28/leveraging-the-brics-network-to-drive-indonesias-ai-strategy.

OECD. *Global Partnership on Artificial Intelligence*. 2024. https://www.oecd.org/en/about/programmes/global-partnership-on-artificial-intelligence.html.

OpenAI. "Announcing the Stargate Project." 2025. https://openai.com/index/announcing-the-stargate-project.

Research and Markets. *Artificial Intelligence in Aerospace & Defense — Global Strategic Business Report*. 2025. https://www.researchandmarkets.com/reports/6042657/artificial-intelligence-in-aerospace-and-defense.

Reuters. "Baidu Says 2nd-Gen Kunlun AI Chips Enter Mass Production." 2021. https://www.reuters.com/technology/baidu-says-2nd-gen-kunlun-ai-chips-enter-mass-production-2021-08-18.

Russo, Lucia, and Noah Oder. "How Countries Are Implementing the OECD Principles for Trustworthy AI." *OECD*, 2023. https://oecd.ai/en/wonk/national-policies-2.

Sanders, Corey. "Microsoft Cloud for Sovereignty: The Most Flexible and Comprehensive Solution for Digital Sovereignty." *Microsoft*, 2022. https://blogs.microsoft.com/blog/2022/07/19/microsoft-cloud-for-sovereignty-the-most-flexible-and-comprehensive-solution-for-digital-sovereignty.

SHEN, Yujia, et al. "Towards Bidirectional Human-AI Alignment: A Systematic Review for Clarifications, Framework, and Future Directions." *ACM Preprint*, 2024. https://arxiv.org/pdf/2406.09264.

Shivakumar, Sujai, Charles Wessner, and Thomas Howell. "Balancing the Ledger: Export Controls on U.S. Chip Technology to China." *CSIS*, 2024. https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china.

Siegmann, Charlotte, and Markus Anderljung. *The Brussels Effect and Artificial Intelligence*. Centre for the Governance of AI, 2022. Shahbaz, Adrian. *The Rise of Digital Authoritarianism*. Freedom House, 2018. https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

Sijarvis. "Compute Governance Literature Review." *LessWrong*, 2024. https://www.lesswrong.com/posts/eLzDLCB68qNoWDRba/compute-governance-literature-review.

Tech-Diplomacy. "What Is Tech Diplomacy?" n.d. https://www.tech-diplomacy.org.https://cdn.governance.ai/Brussels_Effect_GovAI.pdf.

Ünver, H. Akin. *Artificial Intelligence (AI) and Human Rights: Using AI as a Weapon of Repression and Its Impact on Human Rights*. European Parliament, 2024. https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf.

Vergun, David. "DARPA Aims to Develop AI, Autonomy Applications Warfighters Can Trust." *U.S. Department of Defense*, 2024. https://www.defense.gov/News/News-Stories/Article/Article/3722849/darpa-aims-to-develop-ai-autonomy-applications-warfighters-can-trust.

Wang, Maya. "China's Techno-Authoritarianism Has Gone Global." *Human Rights Watch*, 2021. https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global.

Webster, Graham, Rogier Creemers, Elsa Kania, and Paul Triolo. "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)."

Stanford University DigiChina, 2017. https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017.

U.S. Congress. *H.R.4346 — CHIPS and Science Act*. 2021. https://www.congress.gov/bill/117th-congress/house-bill/4346.

U.S. Congress. *H.R.6216 — National Artificial Intelligence Initiative Act of 2020*. 2020. https://www.congress.gov/bill/116th-congress/house-bill/6216.

UN AI Advisory Body. *Governing AI for Humanity: Final Report*. 2024. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf.

UNESCO. *Recommendation on the Ethics of Artificial Intelligence*. 2023. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

United Kingdom, Prime Minister's Office. *AI Safety Summit 2023*. GOV.UK. https://www.gov.uk/government/topical-events/ai-safety-summit-2023.

UNODA. *Lethal Autonomous Weapon Systems (LAWS)*. 2023. https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw.

Authors' bios

Hamza Aarab is a researcher focused on economic diplomacy and emerging technologies. He holds masters and postgraduate degrees in international relations, political science and economic diplomacy, and has worked professionally in IT engineering and digital infrastructure. His research explores how AI and digital technologies shape global governance, financial regulation, and international cooperation.

Parker Bourns is a 3rd Year Political Science and Science, Technology Information Systems, and Public Policy BS/MS Student from the Rochester Institute of Technology. He studies Military Science and plans to commission as a Lieutenant in the United States Army after graduation. As both a Political and Military Scientist, Parker takes great interest in the political ramifications of unconventional warfare and conflict.

Cayla Chun is a senior undergraduate student-athlete at St. Olaf College. A triple major in Political Science, Russian Studies, and Asian Studies with a concentration in International Relations, Chun's interests lie in government and intelligence.

Andrew Ellis is a student at Texas A&M University, pursuing a bachelors in History. His research and program involvement focuses on international affairs and public service. He enjoys experiencing new things and taking on new challenges. He would also like to thank Civitas University faculty for their generous guidance and hospitality.

Medha Kalidas is an undergraduate at the University of California, Berkeley, double majoring in Cognitive Science and Global Studies, focusing on Peace and Conflict of Europe and Russia. She has a strong background in

security studies, behavioral science, and digital threat analysis through her work with Berkeley School of Information and Project RISHI. A lover of language learning and travel, Medha is pursuing a career in intelligence and service, with interests in counterterrorism.

Catherine Kerckhove is a rising junior at Iowa State University majoring in Criminal Justice and International Studies with an emphasis on conflict in the Middle East and Africa. She is also working on a minor in Political Science. She hopes to earn her Master's degree in International Security Policy and continue her Arabic language courses to fluency. Her career aspirations are intelligence work or security advising in the future.

Kenneth McDaniel is a University Student at the University of Texas at Austin completing his International Relations and Global Studies by Summer 2025.

Tanvi Merianda is a pre-medical student at The University of Texas at Austin pursuing a degree in International Relations and Global Studies with a concentration in International Security. She hopes to work in humanitarian aid within the Middle East and Central Asia. Additionally, she is interested in studying human rights, gender-based violence and humanitarian crisis response. Firm in her belief that speaking someone's language is one of the best ways to bridge cultural divides, she speaks Hindi, Kannada, Urdu, Arabic, and Russian — and hopes to learn many more.

Alexander Mock is a student currently enrolled as a junior at East Carolina University with a major in Security Studies currently in progress. He is also in the process of receiving minors in both History and Aerospace Studies. He has taken part in the school sanctioned Security Studies Club for two semesters. He has made the Honor Roll in both of his semesters attending ECU with a current Grade Point Average of 3.01. He possesses a rather niche interest in aircraft weapons systems and radar capabilities. His goal for a post graduation job position is securing employment as an intelligence analyst with an agency which works with or for the United States Air Force in identifying aircraft to fulfill his niche.

Ashlyn Mundell is currently an undergraduate student at Northern Arizona University studying criminology & criminal justice, sociology, and emergency management. Her interest in researching domestic surveillance stems from the asymmetrical power differential present in modern political and social contexts.

Irwin Salazar is a career diplomat from Mexico who focuses on international security, digital governance and multilateral negotiations. Throughout his career he has served as a representative of Mexico in foreign countries while developing programs for cultural diplomacy, international cooperation and human rights. His present research investigates how AI technology and other emerging systems transform diplomatic practices and institutions worldwide.

Audra Soni has completed her freshman year at Georgetown University. She plans to study Science, Technology, and International Affairs in the School of Foreign Service. At Georgetown, she is part of the Corp, a student-run coffee shop; club lacrosse; The Hoya newspaper; Active Minds, a mental health advocacy club; and Alpha Kappa Psi, a pre-professional business fraternity. In her free time, she loves playing lacrosse, traveling, following politics, doing puzzles, reading novels, and spending time with loved ones. Her research interests are global stability and humanitarian efforts relating to the Russian invasion of Ukraine and other Eastern European diplomatic challenges.

We are pleased to present the eighth volume, bringing together a unique series of papers by talented young researchers from both sides of the Atlantic. This publication includes articles by "Security and Society in the Information Age" program participants and papers by International Security Studies students, presenting the transatlantic youth perspectives on security issues.

The "Security and Society in the Information Age" program, composed of a summer school and semester/academic year study abroad opportunities, was designed and launched jointly in 2015 by two partners: SRAS (USA) — a leading study abroad facilitator, and Civitas University (formerly: Collegium Civitas) — a leading non-public university in Warsaw, Poland.

The 2025 curriculum focused on new and emerging threats, including the regional and global consequences of the Russian invasion of Ukraine and the broader interconnectedness of international conflicts, with special attention to developments in the Middle East. During the 2025 summer school 19 participants — students of leading American colleges and universities — engaged deeply with critical topics such as terrorism and counterterrorism strategies, state sponsorship of terrorism, radicalization and prevention, public diplomacy, private military companies, international humanitarian law, peacebuilding and post-conflict reconstruction, hybrid threats and disinformation, and cybersecurity.

Those topics are reflected in this book. In addition, students and alums of the International Security Studies master's degree program at Civitas University were invited to submit papers to this volume. By gathering youth perspectives on security issues, from Europe and the US, with this book, we hope to contribute to strengthening the transatlantic bonds in security research, primarily among the new generation of researchers.

ISBN 978-83-66386-60-0

9 788366 386600