BITSMUN

GOA '26

BITSMUN GOA 2026

UNITED NATIONS HUMAN RIGHTS COUNCIL

Background Guide

Agenda:

1. Integrating IHRL Standards into Customary IHL for Non-State Armed Groups in Hybrid Warfare
2. Ensuring accountability and rights protection in the use of digital surveillance and monitoring technologies

I. Letter from the Executive Board

Dear Delegates,

It gives us great honour and immense pleasure to welcome you all to the United Nations Human Rights Council at BITSMUN Goa, 2026. As representatives of member nations of the UNHRC, you are tasked towards debating, deliberating, and reaching a consensus on the agenda at hand.

As you are aware, the committee will be discussing one of the two agendas set forth in the background guide which are: "Integrating IHRL Standards into Customary IHL for Non-State Armed Groups in Hybrid Warfare" and "Ensuring accountability and human rights protection in the use of digital surveillance and monitoring technologies". This background guide has been designed to help you get started on your research. However, this document shouldn't be your only source of research. Building upon the outlook presented by this guide, you are expected to carry out your own research through authentic sources and make sure to engage in comprehensive and pragmatic debate throughout the sessions. The background guide has been drafted thoroughly to ensure a holistic overview of the agenda which can help you better understand the crux of the issues at hand and how to direct the committee towards the desirable direction in order to achieve consensus and address the issues being discussed in committee.

The Executive Board will not interfere in the flow of debate unless absolutely required. Therefore, the onus to ensure that the committee does not stagnate lies on the delegates. We strongly believe that with good research, the delegates will be able to steer the committee in the right direction.

That being said, we sincerely hope that all delegates maintain the highest standards of decorum and be on their best behaviour during the days of the conference. Remember, you must emulate the behaviour of a diplomat representing your country to the best of your ability.

Please do not hesitate to get in touch with the Executive Board at any time before or during the conference in case you have any queries about the agendas or the rules of procedure. Further, we have added one addendum to this letter that talks about the nature of evidence entailed in this simulation.

We request that the delegates not view this conference as a zero-sum game. Model UN conferences are collaborative rather than competitive and we would like to

keep this spirit alive during our committee. Our goal isn't to solve the world's problems in three days, but rather to educate ourselves about them, thereby ensuring that we go on to become a generation of sensitized leaders, equipped with the skills and desire to make our world a better place.

With that being said, we wish you all good luck and eagerly look forward to the conference.

Warm regards,

Kshitij Saha- Chairperson (kshitijgsaha@gmail.com)

Anamika - Co-Vice Chairperson (anamikauralath@gmail.com)

Paarth P V - Co-Vice Chairperson

Addendum: Nature and Proof of Evidence

Documents from the following sources will be considered as credible proof for any allegations made in committee or statements that require verification:

1. Reuters: Appropriate Documents and articles from Reuters News agency will be used to corroborate or refute controversial statements made in committee.
2. UN Documents: Documents by all UN agencies will be considered sufficient proof. Reports from all UN bodies including treaty-based bodies will also be accepted.
3. National Government Reports: Government Reports of a given country used to corroborate an allegation on the same aforementioned country will be accepted as proof. The documents stated above will hold a binding nature of establishment.
4. Other sources like Wikipedia, Amnesty International, or newspapers like the Guardian, so on and so forth will not be accepted as credible proof; but may be used for better understanding of any issue and even be brought up in debate, if the information given in such sources is in line with the beliefs of a government or a delegate.

II. **Beginners' Guide to Model UN**

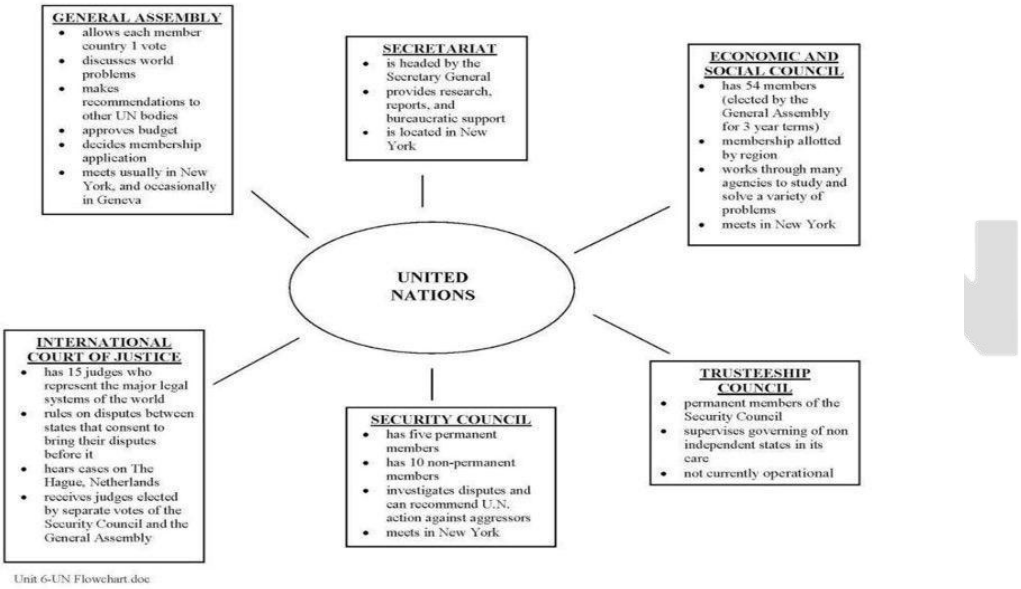
Question 1: What are the United Nations?

The United Nations is an international organization founded in 1945 to maintain international peace and security, developing friendly relations among nations and promoting social progress, better living standards and human rights by 51 countries. The United Nations has 6 principal organs.

The UN has 4 main purposes:

- To maintain peace throughout the world;
- To develop friendly relations among nations;
- To help nations work together to improve the lives of poor people, to conquer hunger, disease and illiteracy, and to encourage respect for each other's rights and freedoms;
- To be a centre for harmonizing the actions of nations to achieve these goals

PRINCIPLE ORGANS OF UNITED NATIONS



Question: How to prepare for the Model United Nations overview?

General Research and Preparation guidelines

There are three consistently significant parts of representative planning. They are: useful; meaningful; and positional planning. Practical readiness outfits the

representatives with essential apparatuses, including a comprehension of the guidelines important to act in board of trustees. The meaningful component gives preparation of explicit data on the subject regions. At long last, positional planning requires the understudies to embrace viewpoints that are not their own. In light of this, the EB gives three instruments to help you: this Guide to Delegate Preparation, Background Guides, and position papers. Together, these will guarantee you will be prepared for the gathering. Past perusing and understanding the material we have given, the more pragmatic experience you can gain through banter, goal composing, making introductions, and so forth, the more ready you will be.

Meaningful Preparation

The Background Guides are a consequence of broad exploration and exertion with respect to the Executive Board and are the establishment of considerable groundwork for every advisory group. We recommend that you read them, talk about them, and read them once more. On the off chance that an agent has not perused and ingested the data in the Background Guide, the person won't contribute adequately to the board. An ambitious beginning on the Background Guides will empower you to completely comprehend the subjects and start to tissue out your own thoughts. Advise yourself that you should go about as policymakers, dissecting and shaping the data you have gotten into arrangements and goals. Conversations with different representatives will likewise assist you with fostering your thoughts. While the Background Guide will give a large portion of your meaningful readiness, autonomous exploration is valuable, fulfilling and important for a fruitful gathering.

Positional Preparation

We expect representatives to receive the situation of a particular country all through the UN reproduction. This is a vital component of the "global" experience of a model UN as it powers representatives to analyse the points of view, issues, and arrangements of one more country at an exceptionally major level. It is additionally quite possibly the most troublesome parts of MUN on the grounds that understudies should go up against natural inclinations of their own public viewpoints and authentic data. The position papers are the focal point of positional planning before the meeting. Albeit generally short, we request that you invest energy and exertion on investigating and keeping in touch with them.

Materials arranged by the EB are not intended to fill in for your individual exploration. All things being equal, they ought to give a beginning stage, motivating you to ask yourself inquiries about the current issues. The best-

arranged agents are those that accept the given materials as the start of their exploration and dig further into the theme regions. Past these materials are a large group of data administrations, starting with United Nations sources. UN's assets regularly have ordered measurements, outlines, and charts which you may discover supportive in understanding the issues. Most UN report communities convey records of UN gatherings; maybe the most ideal approach to comprehend your nation's position is to see it iterated by its diplomat.

Explicit assets to research include:

- Yearbook of the United Nations: The Yearbook is a decent beginning stage for your examination. The Yearbook will furnish you with general data on what has been done on your theme during a specific year. It likewise gives exceptionally accommodating references to past articles and goals.
- United Nations Chronicle: This magazine gives you general data on the procedures of the UN. Watch out for exceptional reports on your theme region, which will advise you about the point and countries' situations on it.
- UN Document Index: This record for all UN reports comes in three distinct renditions: UNDI (1950-1973), UNDEX (1970-1978), and UNODC (1979-present). Contingent upon which of the three you are utilizing, you will track down a subject record, a nation file, and an alphanumeric rundown of all reports distributed (this is helpful in light of the fact that each panel has its own novel alphanumeric prefix and accordingly you can track down every one of the records put out by a board of trustees during a specific year paying little heed to the particular theme.
- UN Resolutions: This arrangement is both significant and extremely simple to utilize. The record is aggregate from 1946, which implies that you need just check the most current list to track down every one of the goals on your point that the UN has at any point passed.
- Other UN Sources: Depending on the subject, there may be extra pertinent UN sources. Check for books and exceptional reports put out by the WHO. Past United Nations sources, notwithstanding, are general wellsprings of data. Explore your school and nearby libraries. Look at diaries, periodicals, and papers for more current sources. Remember to ask the curators for help.
- Books: Up-to-date books are probably going to give you a profundity and exactness that is hopeless from UN sources or periodicals. Try to check library postings for bound materials. Book research, in any case, can take a decent arrangement of time, so use prudence when choose books.
- Periodicals: Periodicals are valuable for straightforward, current data on points (the Reader's Guide to Periodical Literature and InfoTrack fill in as a record for these materials). Try not to anticipate that they should supply you with the profundity of data you will require for the Conference.
- People: A regularly ignored source; individuals can help you extraordinarily in your exploration. A few groups to remember are: bookkeepers, individual agents, personnel counsellors, and your board of trustees' Director, Moderator, and Assistant Directors. Not exclusively can these individuals

help you discover what you are searching for, yet they may likewise suggest new sources that you had not thought of. Try not to spare a moment to call or email your advisory group Director.

- Embassies and Consular Offices: Contact the government office or consular office of the country that you are addressing. These spots are happy to help you in your exploration via mailing factual information and other unclassified data. RESEARCH AID

(This is just a suggested pattern, you can research your way, individual differences make us all special but these suggestions may aid you in understanding where to start)

1. Start from knowing
    a. `United Nations
    b. Your committee
    c. Mandate of the committee (functions and power)
    d. Bodies it works with
    e. Final result of your committee
    f. Funding channels

2. Know your Agenda
    a. Historical background
    b. Current trends
    c. Future aims
    d. International legal instruments

3. Within the agenda cover the following areas
    a. Political
    b. Economic
    c. Social
    d. Technology and its role
    e. Arms and army strength
    f. Legalities
    g. Impacts and implications of (a-f) on historical background, current trends, future aims and international legal instruments.

Note: International legal instruments are applicable on Nations for them to reach individuals they should be incorporated in domestic law as individuals are subjects of it i.e. domestic law is applicable on citizens. So, it is crucial to understand the relationship between the two and bridge and the gap for effective implementation.

4. Know your country

a. Historical background, Current trends, Future aims of the agenda from your country's perspective.
b. Political, Economic, Social, Technology and its role, Arms and army strength and Legal aspect related situation in your nation. (emphasis on High value resources, crisis, support services, governance, political system and administrative conditions)
c. Membership and participation in regional organizations
d. International organizations other than UN
e. Allies and non-allies (friends and enemies) of your nations

NOTE: Research alone is not enough, as it would be simply reading out from the internet what is needed is to "Analyse" i.e. to present your understanding of the research.

III. Overview of the Committee

A. Introduction to the Human Rights Council

Human rights are inalienable entitlements established not by law, but by human birthright, and the history of human rights has been shaped by all major world events and by the struggle for dignity, freedom, and equality everywhere. However, human rights gained formal recognition only after the inception of the United Nations (UN) and the establishment of the UN Charter. In its subsequent attempt to "promote and encourage respect for human rights and fundamental freedoms for all", the UN established specific Charter-based and Treaty-based mechanisms. Charter-based mechanisms derive from provisions of the charter whereas treaty-based mechanisms include the international conventions and covenants, along with their respective treaty bodies, that aim to promote, protect, and safeguard the human rights of all individuals. The Human Rights Council (HRC) is a UN subsidiary body established under the UN Charter. It is the main organ of the United Nations (UN) responsible for strengthening the promotion and protection of human rights around the globe.

The HRC is mandated to respond to urgent human rights crises and make pertinent recommendations for the cessation of human rights violations prevalent around the world. It has a global scope and works to promote all human rights and uphold the integrity of International Conventions and Covenants on Human Rights. As a part of the treaty-based mechanisms, the Universal Declaration for Human Rights (UDHR) was adopted by the General Assembly as a "common standard of achievement" for all peoples and countries to pursue the protection and promotion of human rights. After decades of standing alone as the only landmark document on human rights, it was joined by the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the International Covenant on Civil and Political Rights (ICCPR) and its two Optional Protocols to comprise the International Bill of Rights.

To further facilitate the implementation of the UDHR, the UN Secretariat established a UN department responsible for overseeing its human rights program. This department, known as the Centre for Human Rights, expanded its reach in the 1980s and moved from New York to Geneva. In 1993, at the World Conference on Human Rights, Member States created the Office of the UN High Commissioner for Human Rights (OHCHR) with the responsibility of coordinating the human rights agenda across all intergovernmental agencies and departments within the UN. OHCHR is responsible for the substantive, logistical, and administrative needs of all UN human rights mechanisms, including core treaty-based bodies, thematic working groups, and the HRC.

Source: https://www.minorityrightscourse.org/mod/page/view.php?id=1626

B. Partnerships

The HRC continues to spearhead global efforts in upholding human rights by forging partnerships and providing assistance to non-governmental organizations (NGOs), National Human Rights Institutions (NHRIs) of member nations, and other civil society actors playing a role in safeguarding and promoting human rights. These partnerships facilitate many of the HRC's major initiatives, including providing humanitarian assistance and aid through programs or frameworks targeting groups deprived of their access to fundamental human rights and freedoms. NGOs that have received Economic and Social Council (ECOSOC) consultative status and NHRIs can directly address HRC during discussions and debates and inform it of situations occurring in their home states. Groups and NGOs that have not achieved ECOSOC consultative status can also provide written documents on a Member State as part of the Universal Periodic Review (UPR) which serves to assess the human rights situations in all United Nations Member States.

C. Mandate and Functions

The HRC possesses a unique and comprehensive mandate outlined in General Assembly resolution 60/251 of 2006 on the "Human Rights Council" and guided by the principles of "universality, impartiality, objectivity and non-selectivity, constructive international dialogue, and cooperation." The General Assembly mandates the HRC to promote universal respect for human rights and fundamental freedoms; to address and provide recommendations on all, particularly grave and systematic violations of human rights, and to promote an effective system of coordination within the UN system with respect to human rights issues.

In 2007, the HRC adopted resolution 5/1 on "institution-building," which established mechanisms and structures to guide its program of work, rules of procedure, and other operational functions. The resolution also established the format for the Special Procedures, the UPR, and the Complaint Procedure, which comprise the main powers of the HRC.

Special Procedures are mechanisms that enable independent parties to report, monitor, and advise on country-specific or thematic situations for the HRC. Each investigation has a mandate and a mandate holder, who is typically a Special Rapporteur, an independent expert, or a working group, to carry out the investigation. Special Procedures are empowered to undertake country or field visits, with the support of Office of the High Commissioner of Human Rights (OHCHR), and to bring specific cases and concerns to the attention of Member States. They can send communications detailing accusations of violations or

abuses of human rights, engage in advocacy efforts, and offer technical assistance when possible.

D. Universal Periodic Review

The Universal Periodic Review (UPR) is a unique process conducted by the United Nations (UN) Human Rights Council. It involves the assessment of the human rights records of all UN Member States. The UPR was established in 2006 with the aim of ensuring that every country's human rights situation is scrutinized by both the international community and the country itself.

I. Agenda 1

1. Overview of the Agenda

The agenda "Integrating IHRL Standards into Customary IHL for Non-State Armed Groups in Hybrid Warfare" asks how civilian protection can be strengthened when organized armed groups are major conflict actors and when hostilities are blended with proxies, deniable operations, and information/cyber tactics commonly discussed as *hybrid warfare*.

A key reason the agenda centres on customary IHL is that customary international humanitarian law consists of rules derived from "a general practice accepted as law" and exists independently of treaty law, making it a critical baseline in non-international armed conflicts where treaty coverage is comparatively limited. The ICRC's customary IHL resources are used as legal references in both international and non-international armed conflicts and are designed to consolidate rules and practice for use by courts, tribunals and international organizations.

The agenda also explicitly incorporates a justice dimension: hybrid warfare increasingly produces hybrid accountability gaps, where NSAGs commit serious IHL/IHRL-type violations (killing, torture/ill-treatment, hostage-taking, arbitrary deprivation of liberty, discriminatory persecution), yet domestic enforcement is often impossible because states may lack territorial control, investigative reach, or political capacity. This has led to growing reliance on hybrid justice approaches—combinations of national prosecutions, specialized chambers, international support, and UN-mandated investigative mechanisms—to document violations and enable future penalization and remedies.

Finally, "integration" in this agenda does not mean collapsing IHL into IHRL or claiming NSAGs automatically become parties to human rights treaties. Instead, it means using IHRL standards to help interpret and strengthen customary IHL concepts that already bind all parties in NIAC—especially humane treatment and fundamental judicial guarantees—and aligning accountability pathways so NSAG violations do not persist with impunity.

2. Key Concepts and Definitions

Customary IHL: The ICRC explains customary IHL as rules coming from "a general practice accepted as law," existing independently of treaties, and forming part of the law applicable in armed conflict. The ICRC also highlights that its customary IHL study and database aim to identify a "common core" of rules binding on all parties and that the database allows monitoring and evaluation of further developments of customary IHL over time.

IHRL and armed conflict: OHCHR's guidance emphasizes that human rights law continues to apply in armed conflict and that human rights law and IHL are complementary and mutually reinforcing, with IHL sometimes operating as lex specialis in particular contexts. This agenda uses that framing to ask which IHRL standards (for example, basic due process and non-discrimination) can inform how customary IHL is applied to NSAG conduct in NIAC.

NSAGs: For this BG, NSAGs are organized non-state armed groups party to NIACs, which ICRC guidance treats as bound by common Article 3, customary IHL, and (where applicable) Additional Protocol II. The agenda is particularly concerned with NSAGs exercising de facto authority because their governance functions (detention, "courts," policing, information control) generate rights-type harms and create acute needs for enforceable minimum standards.

Hybrid warfare and hybrid justice: Hybrid warfare is used here to capture the blending of conventional violence with proxies, deniability, and non-kinetic tools (including information operations) that complicate both legal classification and enforcement. "Hybrid justice" refers to mixed accountability approaches—using combinations of domestic and international tools (including evidence-preservation and investigative mechanisms) to enable prosecutions and remedies where purely domestic enforcement against NSAGs is not feasible.

3. Scope and Focus of the Discussion

Legally, the agenda concentrates on non-international armed conflict settings where customary IHL forms a central baseline and where organized NSAGs are capable of sustaining hostilities and administering control over civilians. It also recognizes that hybrid warfare patterns can internationalize or complicate NIACs—through proxy control dynamics and cross-border support—creating difficult "grey zone" enforcement conditions even when the humanitarian consequences are severe.

Substantively, the focus is on protections most relevant to civilian life under NSAG influence: humane treatment; safeguards around deprivation of liberty; minimum judicial guarantees; and protection against discriminatory coercion, including abuses linked to information control and intimidation. The scope also includes post-conflict and transition phases where accountability choices are made—whether through domestic courts, special chambers, hybrid tribunals, or internationally supported investigative pathways—because the credibility of legal standards depends on whether violations can realistically be penalized.

Politically, the committee must balance two constraints: strengthening compliance expectations for NSAGs without conferring political recognition, and designing accountability pathways that do not depend on idealized state capacity where none exists. The agenda therefore invites operationally realistic proposals that link standards, monitoring, documentation, and justice mechanisms into a coherent protection architecture.

4. Relevance to UNHRC Mandate

OHCHR's framework on human rights in armed conflict underlines that human rights protections remain relevant during conflict and that human rights law and IHL are complementary and mutually reinforcing, providing a normative basis for UNHRC engagement on how protections should be applied in war. Because hybrid conflicts routinely involve gross violations—often by NSAGs and their sponsors—the Human Rights Council's fact-finding, reporting, and recommendation functions are directly engaged, particularly where domestic oversight is absent.

UNHRC-mandated commissions of inquiry and fact-finding missions are a key bridge between protection and accountability because they investigate patterns of violations, preserve records, and can recommend justice pathways and standards alignment. In addition, the Council's thematic work can clarify minimum standards and press states to "ensure respect" for IHL, including by influencing armed groups over whom they have leverage—an approach consistent with ICRC discussions of respect and ensuring respect in NIAC.

5. Problem Statement: Impunity & Enforcement Gap

ICRC guidance notes that armed groups party to NIACs are bound by common Article 3 and customary IHL, and it discusses practical challenges in increasing respect for IHL in such conflicts, including the need for actors with influence to intervene with parties violating IHL. Yet in many hybrid warfare settings, enforcement against NSAGs fails because state institutions cannot safely investigate, arrest, prosecute, or protect witnesses in territories under NSAG control or in fragmented governance environments.

This creates a structural accountability gap: serious violations persist, victims lack remedies, and compliance incentives remain weak—especially where proxy sponsorship and deniability complicate attribution and political action. The agenda therefore treats accountability as integral to legal integration: clarifying standards (IHRL-informed customary IHL) must be paired with credible "hybrid justice" pathways—evidence preservation, specialized chambers, hybrid tribunals where appropriate, and cross-border cooperation—so NSAG violations do not remain effectively cost-free.

II. Historical Background

1. Development of IHL in NIAC and Rise of Customary IHL Reliance

Modern international humanitarian law (IHL) was historically designed around inter-State war, leaving internal conflicts with comparatively fewer treaty rules for decades. In non-international armed conflicts (NIACs), the treaty baseline is often described as "rudimentary," with Common Article 3 and Additional Protocol II of the Geneva Conventions providing core protections but not a full conduct-of-hostilities code comparable to international armed conflict frameworks.

This gap is a major reason customary IHL became so central to NIAC regulation. The ICRC's *Customary International Humanitarian Law, Volume I: Rules* explicitly notes that customary rules—sometimes referred to as "general international law"—bind all States and, where relevant, "all parties to the conflict," without requiring formal adherence to a treaty. It also highlights that state practice often goes beyond what was accepted in diplomatic conferences and that "the essence of customary rules on the conduct of hostilities applies to all armed conflicts, international and non-international."

As a result, much of the practical law that constrains NSAG conduct in NIAC—especially beyond the minimum floor of Common Article 3—has been articulated through customary IHL as identified and systematized in studies and reflected in practice. This historical reliance on custom is what makes today's "integration" debate meaningful: if customary IHL is a living body of law derived from practice and accepted legal obligation, then sustained interpretation (including through IHRL concepts) and evolving practice can influence how protections are understood and applied in NIAC settings where NSAGs are key actors.

2. Expansion of IHRL Application in Armed Conflict

Parallel to the rise of customary IHL's importance in NIAC, UN practice increasingly emphasized that international human rights law (IHRL) does not "switch off" in wartime. OHCHR's guidance explains that human rights law and IHL are "complementary and mutually reinforcing" bodies of law for protecting persons in armed conflict and that understanding their relationship is crucial for applying protections effectively.

This relationship has often been debated through interpretive approaches like *lex specialis* (where more specialized rules may guide interpretation in particular contexts) while maintaining that human rights obligations remain relevant, especially for protections around deprivation of liberty, fair trial, and humane treatment. Historically, this mattered most for state conduct; however, as NSAGs began exercising de facto authority—running detention systems, imposing "courts," controlling movement and information—the practical need to translate IHRL-type minima into expectations for armed-group conduct became more pronounced, particularly where IHL rules are framed at a higher level of generality.

Over time, the doctrinal move toward complementarity helped create space for the present agenda: rather than treating IHL and IHRL as competing regimes, UN and humanitarian policy discussions increasingly treat them as mutually relevant lenses for civilian protection, including for "hybrid" harm patterns (coercion,

intimidation, information control) that do not always look like classic battlefield conduct but still deeply affect life, security, and dignity.

3. NSAG Commitments and Engagement Approaches

A key historical development in NIAC practice has been the growth of pragmatic engagement tools aimed at increasing compliance by NSAGs without changing their legal status. The ICRC's work on "Increasing Respect for IHL in Non-International Armed Conflicts" emphasizes special agreements contemplated by Common Article 3 as a mechanism for parties to NIAC to make explicit commitments to comply with humanitarian law. The same ICRC publication stresses that Common Article 3 explicitly provides that concluding such special agreements "will in no way" affect the legal status of the parties, addressing a core political concern about legitimization.

Historically, special agreements and unilateral declarations served multiple functions: they clarified applicable rules, enabled structured follow-up when violations occurred, and created a concrete basis on which humanitarian actors could make legal representations and demand accountability. The ICRC also notes examples of special agreements negotiated in Yemen (1962) and Nigeria (1967), illustrating that these tools have long been part of the NIAC compliance landscape rather than a recent innovation.

This evolution is relevant because it shows "integration" is not only a theoretical question about norms; it is also about how norms are translated into operational commitments by NSAGs and how those commitments become leverage points for monitoring, dialogue, and, where feasible, penal consequences. It also demonstrates that mechanisms short of recognition—codes of conduct, declarations, special agreements—can be historically grounded pathways for raising expectations, including for IHRL-informed standards around detention, treatment, and judicial guarantees.

4. Evolution of Accountability for NSAG Violations (including "hybrid justice")

As conflicts increasingly involved NSAGs committing systematic abuses, international policy debates began to highlight the accountability deficit as a central protection challenge. UN Secretary-General reporting on the protection of civilians has emphasized that enhancing protection requires not only compliance but also accountability for violations, including in relation to non-State armed groups, and it has noted that engagement with armed groups—while politically sensitive—can be crucial to reducing civilian casualties and enabling humanitarian protection.

At the justice end of the spectrum, the post-Cold War period saw the development of international and hybrid accountability pathways (international tribunals, hybrid courts, specialized chambers) designed in part to respond to domestic incapacity or unwillingness to prosecute serious crimes in post-conflict environments. While this background guide will later address mechanisms in detail, the historical point is that "hybrid justice" models emerged precisely because purely domestic enforcement often fails after mass atrocities—whether due to destroyed

institutions, political capture, or ongoing insecurity—conditions that frequently also apply to NSAG crimes.

In parallel, investigative and documentation mechanisms became more prominent as bridges between conflict-time violations and future justice. The Human Rights Council's practice of establishing commissions of inquiry and fact-finding missions reflects this evolution, as these bodies document patterns of violations and can help preserve factual records relevant to later prosecutions and accountability options.

5. Hybrid Warfare as a Legal Stress-Test (Classification, Deniability, Enforcement)

Finally, the historical emergence of "hybrid warfare" debates reflect a growing recognition that modern conflict strategies deliberately exploit seams between legal regimes and enforcement systems. When force is exerted through proxies, deniable support, and non-kinetic tools such as information operations, it can become harder to classify conflicts, attribute conduct, and trigger timely accountability—especially when NSAGs are empowered by external support yet shielded by plausible deniability.

These dynamics intensify the very problems that prompted earlier innovations in customary IHL articulation and NSAG engagement, while also amplifying the need for effective accountability pathways. In other words, hybrid warfare is not only a tactical blend; it is historically a stress-test for the entire protection system—rules, interpretation, compliance tools, and justice mechanisms—because it can preserve *impunity* even when harms are severe and well documented.

III. Contemporary Landscape

1. Hybrid Warfare Threat Profile

Contemporary armed conflict is increasingly shaped by a blend of kinetic violence and non-kinetic tools—especially disinformation, polarization, and technology-enabled influence—which can directly affect civilian safety and access to protection. UNDP's 2024 trends material highlights how "fake news" and polarization in a hyper-connected digital world weaken trust in institutions and degrade social cohesion, conditions that can aggravate conflict dynamics and civilian vulnerability.

In hybrid warfare settings, civilians are often targeted not only through direct attacks but also through intimidation, coercion, and information control that undermines their ability to seek safety, humanitarian assistance, or justice. This expands the civilian-harm "battle space" beyond traditional frontlines and makes it harder for existing protection and accountability tools to identify who is responsible for harm when tactics are deniable, distributed across proxies, or executed through digital ecosystems.

For UNHRC purposes, the relevance of this threat profile is that hybrid tactics can generate patterns of harm that resemble core IHRL violations—arbitrary deprivation of life, torture/ill-treatment, arbitrary detention, persecution and discrimination—while also complicating the evidentiary and jurisdictional pathways required to enforce IHL and penalize NSAG violations.

2. NSAG Governance and "Shadow State" Functions

A defining feature of the contemporary landscape is that many NSAGs do not operate solely as mobile armed bands; they also administer territory and populations, exercising coercive power through policing, taxation, "courts," checkpoints, censorship, and detention. Detention is particularly significant because it places individuals under an armed group's control and triggers minimum protections grounded in IHL (humane treatment and fundamental guarantees), while also raising IHRL-type concerns around arbitrariness, due process, and remedies.

The ICRC has recently emphasized the reality and seriousness of detention by NSAGs, noting that public reports and judgments are "full of accounts of egregious crimes against detainees held by State and non-State parties" and that preventing and stopping such violations requires renewed efforts, including practical engagement to translate legal obligations into implementable measures. The ICRC's approach described their highlights both denunciation/accountability and confidential dialogue as pathways to improve detainee protection, illustrating the dual "compliance + accountability" logic that also underpins this agenda.

When NSAGs run governance structures, the protection problem is no longer limited to "conduct of hostilities"; it includes how civilians live under coercive rule—how they are tried, punished, displaced, surveyed, or denied services based on identity or perceived disloyalty. This governance reality is why integrating IHRL standards into the interpretation and evolution of customary IHL is increasingly

discussed as a way to better articulate minimum guarantees applicable in NIAC environments dominated by NSAG authority.

3. Key Human Rights Pressure Points

The most recurring pressure point is deprivation of liberty and the surrounding "justice" ecosystem: who can detain, for what reasons, under what procedures, and with what safeguards against torture, disappearance, and summary punishment. The ICRC specifically recalls that humane treatment and the absolute prohibition of violence to life and person are among the most elementary rules of armed conflict law, yet these rules are "too often" not respected, with reports cataloguing physical, sexual, and psychological violence against detainees.

A second major pressure point is information control, including disinformation and propaganda dynamics that inflame hostility, enable persecution, or suppress civic space and humanitarian warning signals. UNDP's trends analysis flags the destabilizing role of digital misinformation and polarization as systemic risks that degrade cohesion and trust, conditions that can worsen both recruitment into violence and the ability of communities to resist coercion. In hybrid warfare, these dynamics can intersect with NSAG rule through forced messaging, intimidation of journalists, restrictions on movement and association, and digitally enabled surveillance of perceived opponents.

A third pressure point is discrimination and identity-based harm (including gendered harm), which hybrid warfare can amplify by using information campaigns and selective violence to fragment communities and normalize abuse. These harms are central to UNHRC's mandate and they often sit at the boundary between IHL's protections (humane treatment, protections for civilians) and IHRL's more detailed equality, dignity, and due process guarantees.

4. Accountability in Practice: Why Violations Go Unpunished

In many theatres, NSAG violations persist with limited penal consequences because domestic institutions cannot investigate and prosecute crimes in areas outside effective state control, cannot safely protect witnesses, or face political constraints and corruption that block impartial justice. Hybrid warfare compounds this by adding proxy relationships, deniable sponsorship, cross-border logistics, and digital evidence trails that are difficult to authenticate and litigate without specialized capacity.

To respond, UN and international practice has increasingly relied on international investigative mechanisms to document patterns of serious violations of both human rights and IHL and to build an evidentiary record for future accountability. OHCHR's guidance on commissions of inquiry and fact-finding missions states that these bodies "gather and verify information," "create an historical record," "provide a basis for further investigations," and have proved valuable in countering impunity by promoting accountability and recommending measures to provide justice and reparation to victims.

This evolution matters for the agenda because it directly links standards to enforcement: integrating IHRL standards into customary IHL for NSAGs is less meaningful if violations remain effectively cost-free, so the contemporary

landscape must be assessed together with the investigative and judicial pipelines that can operationalize accountability in hybrid contexts.

5. Emerging Practice in Documentation and Evidence Preservation

The UNHRC has increasingly mandated investigative bodies not only to report on violations but also to collect, consolidate, analyse, and preserve evidence consistent with best practices "in view of any future legal" proceedings. This reflects a shift toward "accountability-oriented fact-finding," where documentation is structured to meet future evidentiary needs—an approach particularly relevant when NSAG crimes cannot be prosecuted immediately due to security and capacity constraints.

OHCHR's methodological guidance stresses that mandates should enable commissions/missions to operate in line with best-practice fact-finding standards and that these bodies can influence changes in law and practice while assisting accountability and deterrence. For hybrid warfare, where digital footprints and disinformation complicate verification, the move toward systematic recording and preservation is especially significant because it can reduce the "vanishing evidence" problem that has historically shielded NSAG perpetrators and their sponsors from later prosecution.

IV. Legal and Normative Framework

1. Customary IHL Binding on NSAGs

Customary IHL is central to this agenda because it is widely relied upon to "fill gaps left by treaty law" and strengthen protection for victims in today's armed conflicts, especially where NIAC treaty rules are less detailed. The ICRC's customary IHL study and database set out rules that—based on state practice and acceptance as law—apply in both international and non-international armed conflicts, and are intended to provide a usable baseline for courts, tribunals, and international organizations.

For NSAGs in NIAC, the key point is that core customary rules are understood to apply to all parties to the conflict, which is why customary IHL is often treated as the principal "common legal language" for regulating NSAG conduct beyond the minimum treaty floor. This is reinforced by ICRC explanations that the customary nature of "most of the treaty rules applicable in non-international armed conflicts" has been confirmed, and that many rules initially designed for international conflicts also apply in NIAC as customary rules, including principles like distinction and the protection of civilian objects.

In the context of "integration," certain customary rules are especially relevant because they already embed protections that resonate strongly with IHRL. For example, the ICRC's Rule 87 on humane treatment is identified as customary and applicable in both international and non-international armed conflict. This offers a legal hook for interpreting what humane treatment and fundamental guarantees should mean when NSAGs detain, punish, or otherwise exercise coercive control over civilians.

2. IHRL Obligations: State Duties and NSAG Debates

OHCHR guidance emphasizes that human rights law continues to apply during armed conflict and that IHRL and IHL are "complementary and mutually reinforcing" bodies of law. This is crucial for UNHRC work because many abuses in hybrid warfare—arbitrary detention, torture, enforced disappearance, discrimination, repression of expression—fall squarely within the Council's human rights mandate even when the setting is an armed conflict regulated by IHL

As a matter of black-letter international law, states are the primary duty-bearers under human rights treaties, including obligations to prevent, investigate, and remedy violations (and, in many interpretations, to comply with certain obligations extraterritorially when they exercise control). The difficult question—especially salient when NSAGs act as de facto authorities—is how far human-rights-type obligations apply directly to NSAGs, and whether the international system should articulate functional expectations (linked to effective control and governance functions) even if NSAGs are not treaty parties.

This agenda does not require states to agree on a single theory of "NSAGs as full IHRL duty-bearers." Instead, it uses the UN's complementarity approach to ask what minimum IHRL standards should guide the interpretation and evolution of customary IHL obligations that already bind NSAGs (for instance, what "judicial guarantees" are "indispensable," what safeguards reduce arbitrariness in

detention, and what non-discrimination means in practice under armed-group governance).

3. Interface Methods (How Integration Happens)

A core normative task for delegates is selecting an "interface method" that avoids false binaries. OHCHR's armed-conflict guidance explains that IHRL and IHL often reinforce each other, while *lex specialis* may guide analysis where norms overlap and appear to conflict. In practical terms, this means many protection questions are not solved by choosing either IHL or IHRL, but by interpreting applicable rules in a way that preserves the strongest feasible protection—particularly for persons in the power of a party to the conflict.

For this agenda, integration can occur through at least three legally conservative pathways consistent with UN practice. First, interpretive convergence: using IHRL standards to give content to IHL terms that are intentionally general (e.g., humane treatment, dignity, indispensable judicial guarantees). Second, systemic integration: reading customary IHL and IHRL as part of a coherent international legal system when assessing what minimum procedural and substantive safeguards should apply in NIAC detention and punishment contexts. Third, customary evolution: where state practice and opinio juris increasingly reflect IHRL-informed expectations in NIAC contexts, influencing how customary baselines are articulated over time.

This matters acutely for NSAGs because NIAC settings routinely involve armed-group detention and punishment without the institutional checks that exist in stable states. The legal goal is to articulate minimum standards that remain realistic in conflict conditions while still preventing "conflict exceptionalism" from hollowing out the protections civilians are supposed to enjoy.

4. Accountability Law Architecture

Accountability in this agenda operates on multiple tracks: individual criminal responsibility for serious international crimes; state responsibility where states sponsor, direct, or otherwise provide support that facilitates violations; and institutional accountability mechanisms that preserve evidence and recommend pathways for justice and reparations. While the UNHRC is not a criminal court, it is a key factor in the accountability ecosystem because it can mandate investigations, set expectations for compliance, and keep sustained political attention on impunity patterns involving NSAGs and hybrid warfare tactics.ohchr+2

OHCHR's guidance on commissions of inquiry and fact-finding missions states that these bodies counter impunity by promoting accountability, gathering and verifying information, creating an historical record, and providing a basis for further investigations, and that they can recommend measures to provide justice and reparation to victims. This is particularly relevant where NSAG crimes cannot be prosecuted immediately and where evidence may disappear quickly due to insecurity, displacement, or digital manipulation.

The same OHCHR guidance emphasizes that these bodies' work is guided by international standards and methodologies for human rights and IHL fact-finding

and investigations, tying them directly to both bodies of law that this agenda seeks to integrate. In practice, this means UNHRC-mandated investigations can act as "connective tissue" between IHL/IHRL standards and later hybrid justice mechanisms—specialized chambers, hybrid tribunals, or other proceedings—once political and security conditions permit.

5. New Domains and Hybrid Tactics (Cyber/Information; Private Actors)

Hybrid warfare expands coercion into the information environment, making civilian protection dependent not only on battlefield rules but also on constraints relevant to incitement, intimidation, surveillance, and manipulation of information ecosystems. Because these harms can be inflicted without conventional "attacks" and often below traditional conflict thresholds, they test how existing IHL concepts are applied and make IHRL protections—especially around expression, privacy, and non-discrimination—more salient in conflict analysis.

At the same time, the UN system increasingly recognizes that investigative bodies must be designed to capture complex patterns of harm and preserve evidence "in line with best practice methodology," including in contexts where violations span both human rights and IHL. This supports a key theme of the agenda: if hybrid tactics produce hybrid harms, then protection requires both (a) coherent standards (customary IHL informed by IHRL where appropriate) and (b) coherent accountability pipelines capable of handling digital evidence, proxy relationships, and cross-border conduct.

If you want, next is Section V (Core Challenges and Gaps) written in the same depth, including: NIAC threshold manipulation, "legitimization" fears, evidence/attribution barriers in proxy wars, and why accountability and remedies lag far behind the scale of NSAG violations.

V. Core Challenges and Gaps

1. Classification & Threshold Issues

Hybrid warfare strategies often exploit the grey space between internal disturbance, "below-threshold" violence, and fully formed non-international armed conflict (NIAC), complicating when IHL applies and which bodies can credibly invoke IHL-based obligations in real time. These problems become sharper when multiple armed groups operate in parallel, alliances shift, or external actors provide support that "internationalizes" elements of a conflict while leaving other parts functionally internal, making it harder to maintain a stable legal classification for monitoring and accountability.

This matters for the agenda because customary IHL (and the ability to "integrate" IHRL standards into how it is articulated and applied) depends on clear triggering conditions and clear identification of parties to a conflict. When states deny that armed conflict exists—or label all armed-group violence as "terrorism" to avoid the NIAC framework—humanitarian engagement and compliance work can be curtailed, and protection baselines become harder to enforce.

2. Normative Fragmentation

Even where NIAC classification is accepted, the legal landscape is fragmented: NSAGs are clearly bound by Common Article 3 and customary IHL, while states remain the principal duty-bearers under human rights treaties, creating persistent debate over whether and how to frame NSAG conduct through "human rights obligations" as opposed to "humanitarian obligations." This fragmentation can lead to inconsistent messaging—some actors speak purely in IHL terms (humane treatment), others in IHRL terms (arbitrary detention, fair trial)—even though the harms overlap and civilians experience them as one continuum of abuse.

The risk, identified in ICRC challenges discussions, is that contemporary conflict pressures can push norms downward—toward minimal compliance or strategic lawyering—if parties treat the law as a ceiling rather than a protective floor. In hybrid warfare, that pressure is amplified because deniable tactics can be paired with selective legal narratives, enabling parties to dispute applicable law and thereby delay or dilute accountability.

3. Compliance Incentives and "Recognition" Concerns

A recurring political barrier is the fear that engaging NSAGs on legal standards "legitimizes" them. This concern often makes states reluctant to support special agreements or structured compliance dialogues, even though Common Article 3 expressly contemplates special agreements and states that such agreements do not affect the legal status of the parties.

The ICRC and humanitarian actors emphasize that engagement is often necessary to influence armed-group behaviour, typically by addressing the leadership or hierarchy capable of changing practice. Yet hybrid warfare complicates incentives further: some NSAGs are fragmented, profit-driven, or externally sponsored, reducing the internal discipline and reputational incentives that might otherwise make compliance messaging effective.

4. Enforcement and Remedy Deficit (Impunity Gap)

The most persistent gap is enforcement: NSAG violations of IHL and IHRL-type norms frequently go unpunished because domestic authorities cannot safely investigate or prosecute in NSAG-controlled areas, cannot secure custody of suspects, or cannot protect witnesses from retaliation. The Secretary-General's protection-of-civilians reporting has repeatedly stressed that effective protection requires accountability for violations of both IHL and human rights law and has urged measures to address impunity, including commissions of inquiry and prosecution pathways

Even when international mechanisms document abuses, moving from documentation to penalties is slow and politically contested, especially when the NSAG is tied to a state sponsor or when peace negotiations create incentives to trade accountability for short-term stability. This reality drives the "hybrid justice" angle of the agenda: without credible pathways—specialized chambers, hybrid tribunals, universal jurisdiction cooperation, or evidence-preservation bodies—legal integration alone will not change behaviour.

5. Technology-Driven Challenges (Evidence, Attribution, and Digital Harm)

Hybrid warfare increasingly relies on information ecosystems, producing harms through propaganda, incitement, intimidation, and manipulation, often with digital traces that are volatile, falsified, or hard to authenticate. OHCHR's Berkeley Protocol on Digital Open-Source Investigations notes that open-source information has become important for documenting wrongdoing, but investigators and courts have struggled to adapt, and the volume of material plus risks of misattribution create major verification challenges.

These evidentiary challenges intersect directly with accountability for NSAGs: if violations are documented mainly through digital content but cannot be authenticated to evidentiary standards, perpetrators benefit from a modernized impunity shield. The same OHCHR guidance highlights that investigators often lack access to territory and do not have law-enforcement powers, which makes preservation, chain-of-custody, and witness protection even more critical—especially in conflicts involving NSAG control and hybrid tactics.

VI. Hybrid Justice and Accountability Pathways (improved, contextualized with past actions)

1. Evidence preservation: From "reporting" to "case-file building"

Historically, UNHRC commissions of inquiry (COIs) and fact-finding missions (FFMs) were often viewed mainly as *reporting* tools—documenting violations and making recommendations. OHCHR's guidance makes clear, however, that these bodies have also proved valuable in countering impunity by promoting accountability, creating an historical record, and providing a basis for further investigations, while recommending measures to provide justice and reparation to victims.

A key evolution—directly relevant to NSAG impunity in hybrid warfare—is the move toward investigative mandates that explicitly support future prosecutions through evidence preservation and analysis, even when trials are not immediately feasible. This reflects the reality that NSAG-controlled territory, witness intimidation, and ongoing hostilities can block domestic proceedings for years, making evidence pipelines the critical bridge between atrocities and eventual justice.

2. A concrete precedent: the IIMM (Myanmar) as a "hybrid justice" tool

One of the clearest examples of "hybrid justice architecture" created through UNHRC action is the Independent Investigative Mechanism for Myanmar (IIMM), established by the Human Rights Council in 2018. UNOG's description states that the IIMM is mandated to "collect, consolidate, preserve and analyse evidence" and to "prepare files" to facilitate fair and independent criminal proceedings in national, regional, or international courts that have or may have jurisdiction in the future.

This is important for the agenda because it shows a practical model for addressing NSAG (and state) impunity in environments where domestic enforcement is blocked: an independent mechanism preserves evidence to prosecutorial standards while leaving the eventual forum open (domestic courts, universal jurisdiction, regional or international tribunals). The IIMM's public materials emphasize the same logic—preventing evidence from disappearing or being destroyed and enabling future prosecutions for serious international crimes.

3. Methodology for hybrid warfare evidence (digital + denial)

Hybrid warfare expands the evidentiary problem: violence is paired with denial narratives and digital manipulation, and documentation increasingly relies on open-source content, satellite imagery, and user-generated material. OHCHR's Berkeley Protocol responds to this modern reality by providing guidance on professional methodologies and procedures for gathering, analysing, and preserving digital open-source information.

The Berkeley Protocol's launch remarks also emphasize that digital materials must be handled with the same rigor as other evidence—source assessment, protection, corroboration, verification, and standard-of-proof discipline—and that the Protocol is designed so information can later be usable for accountability in courts, vetting,

transitional justice mechanisms, and COIs/FFMs, especially when investigators are denied physical access. For UNHRC delegates, this directly informs what "hybrid justice" must look like in hybrid warfare: not only *collecting* content, but ensuring it is preserved with reliability and security so NSAG perpetrators cannot hide behind information chaos.

4. Domestic prosecutions + specialized chambers (why they often need international scaffolding)

Past conflict settings repeatedly show that the default accountability expectation—domestic investigation and prosecution—breaks down when NSAGs retain territorial control, intimidation capacity, or political leverage after fighting ends. OHCHR's COI/FFM guidance notes that commissions/missions often review judicial and other accountability mechanisms and recommend strengthening legislation and institutions to improve accountability at national or international level, and it observes that "in some instances special domestic accountability mechanisms have been established" to address violations investigated by the commission/mission and give effect to its recommendations.

For this agenda, that history supports a core policy claim: hybrid justice is often necessary not because domestic justice is undesirable, but because it is frequently structurally unable to function in NSAG-heavy conflicts without external support in training, evidence handling, witness protection, and institutional independence. Delegates can therefore argue for UNHRC recommendations that explicitly connect evidence mechanisms (like IIMM-type models) with domestic capacity-building and specialized chambers, so accountability does not stall at the "documentation" stage.

5. Complementary non-judicial accountability (truth, reparations, non-recurrence)

Even strong criminal accountability cannot address all harms in NSAG-intense conflicts, particularly where violations are widespread, victims are massive in number, and many perpetrators cannot realistically be prosecuted. OHCHR's guidance explicitly links commissions/missions to recommendations on justice and reparations and notes that their work can inform more sustainable peacebuilding and reconciliation efforts, which reinforces that hybrid justice ecosystems should be designed to include remedies and guarantees of non-recurrence, not only trials.

VII. Existing International and UN Actions

1. UNHRC tools already used (investigations + evidence for justice)

The Human Rights Council has a long record of creating commissions of inquiry (COIs) and fact-finding missions (FFMs) to investigate serious violations, clarify patterns of abuse, and recommend accountability measures. OHCHR's guidance notes that these mechanisms can counter impunity by promoting accountability, gathering and verifying information, creating an historical record, and providing a basis for further investigations, while recommending measures for justice and reparation to victims.

A major "action precedent" relevant to NSAG impunity is the Council's shift from purely narrative reporting toward mandates that support future prosecutions by preserving and analysing evidence. The most explicit example is the Independent Investigative Mechanism for Myanmar (IIMM), described by UNOG as mandated to "collect, consolidate, preserve and analyse evidence" and "prepare files" to facilitate fair and independent criminal proceedings in national, regional, or international courts. This is directly relevant to hybrid warfare contexts because it shows what the UNHRC can do when domestic enforcement is blocked: build prosecutable case files even without immediate arrests or trials.

2. UN system coordination on civilian protection and accountability

UN Secretary-General reporting on protection of civilians (PoC) has repeatedly framed accountability as a core element of effective civilian protection, including where violations are committed by non-State armed groups, and has emphasized engagement and compliance measures alongside accountability. This PoC framing is important for your agenda because it links the legality question (what standards apply to NSAGs) with the enforcement question (how impunity is reduced), which is the "hybrid justice" dimension.

In practice, UN actions on accountability often involve cross-pillar coordination: UNHRC investigative outputs may later support criminal processes and other accountability avenues, while other UN bodies (including in New York) may apply political pressure, sanctions, or mandate support that shapes enforcement feasibility. The agenda therefore benefits from understanding UNHRC as part of an "accountability ecosystem," rather than as a standalone norm-setter.

3. ICRC action on NIAC compliance and NSAG engagement

The ICRC has developed extensive guidance on increasing respect for IHL in NIAC, including specific discussion of engaging armed groups and the use of special agreements contemplated by Common Article 3. Importantly, the ICRC notes that Common Article 3 explicitly states that special agreements do not affect the legal status of the parties, addressing the concern that compliance engagement equals political recognition.

The ICRC also continues to develop and update resources that systematize customary IHL rules and underpin arguments about the baseline obligations binding all parties. For this agenda, ICRC action provides both the *substantive*

foundation (customary rules) and the *implementation* logic (engagement tools that can work even when enforcement is weak).

4. Methodology and standards for digital evidence (hybrid warfare reality)

A core operational constraint in hybrid warfare is evidentiary: conflict documentation increasingly relies on digital open-source information, but courts and investigators face verification and reliability challenges. OHCHR's Berkeley Protocol was created specifically to provide professional guidance on the collection, verification, and preservation of digital open-source material so it can support accountability processes, including international investigations.

This is an "action" relevant to UNHRC agendas because it has directly influenced how investigations and accountability-oriented mechanisms approach digital evidence, especially when physical access to territory is blocked. For delegates, it offers a concrete basis for operative clauses on evidence standards, chain-of-custody expectations, and safe preservation to enable prosecutions for NSAG violations.

VIII. Case Studies (Real-World anchors)

1. Myanmar — Evidence mechanism for future prosecutions (IIMM)

A leading example of a "hybrid justice" approach created through UNHRC action is the Independent Investigative Mechanism for Myanmar (IIMM), established to bridge the gap between documentation and future criminal trials. UNOG describes the IIMM's mandate as collecting, consolidating, preserving and analysing evidence and preparing files to facilitate fair and independent criminal proceedings in national, regional, or international courts that have or may have jurisdiction.

This is directly relevant to the agenda because it shows how the UN system can respond when perpetrators (including organized armed actors and state-linked forces) operate in an environment of impunity and domestic justice cannot function effectively: create an independent mechanism that preserves evidence now for accountability later. It also sets a model for other hybrid warfare contexts where NSAG crimes are documented but not prosecutable in real time due to territory denial, insecurity, or lack of domestic capacity.

2. Syria — UNHRC fact-finding and persistent impunity (NSAG + state actors)

Syria illustrates the core "hybrid accountability problem" in a long-running NIAC/internationalized conflict: multiple armed actors (state forces, allied forces, and numerous NSAGs) committed serious violations, while the prospect of timely domestic accountability remained minimal. OHCHR's guidance on COIs/FFMs explains that such mechanisms counter impunity by gathering and verifying information, creating an historical record, and providing a basis for further investigations and accountability recommendations—functions that have been central in Syria-type contexts even when prosecutions are politically blocked.

For this agenda, the Syria case anchor is less about a single tribunal and more about the *architecture*: sustained UNHRC investigative work to document patterns of violations (including by NSAGs), paired with later or parallel accountability efforts in other fora, relying heavily on preserved testimony and increasingly on digital evidence.

3. Yemen — NIAC complexity + "special agreements" as compliance tools (NSAG engagement without recognition)

Yemen is a useful anchor for the "integration without recognition" dimension because NIAC compliance discussions have historically included the concept of special agreements (as envisaged by Common Article 3), which the ICRC highlights as a mechanism to enhance compliance in NIAC. The ICRC notes that Common Article 3 expressly provides that the conclusion of special agreements "shall not affect the legal status of the Parties to the conflict," addressing a central political objection that engagement confers legitimacy.

In hybrid conflict environments like Yemen, where multiple armed actors, territorial fragmentation, and external involvement complicate enforcement, such compliance tools matter because they can raise standards and reduce harm even when criminal accountability is delayed. For delegates, Yemen functions as the case hook for operationalizing minimum standards—especially around treatment

of persons in custody and humanitarian access—through structured commitments while keeping legal status unchanged.

4. NSAG detention and "courts" — translating law to practice (cross-cutting case pattern)

A recurring real-world pattern across multiple conflicts (rather than one single country) is NSAG detention paired with armed-group "justice" practices—interrogations, punishments, and ad hoc courts—creating acute risk of torture, ill-treatment, enforced disappearance, and summary punishment. The ICRC stresses that public reports and judgments contain extensive accounts of egregious crimes against detainees held by both state and non-state parties and argues that preventing such violations requires renewed efforts to translate legal rules into practical measures.

This pattern is central to the agenda because detention is where IHL's customary/fundamental guarantees and IHRL's due-process logic most visibly intersect in civilian experience. It also highlights why "integration" cannot be purely theoretical: minimum guarantees must be communicable to NSAG command structures, monitorable by independent actors, and ultimately enforceable through accountability pathways when violations occur.

5. Hybrid warfare's information dimension — polarization, misinformation, and civilian harm

Hybrid warfare also operates through information environments that can drive violence, enable persecution, and undermine civilian protection by eroding trust and inflaming divisions. UNDP's trends work highlights that misinformation ("fake news") and polarization in a hyperconnected digital world contribute to weakening trust in institutions and degrading social cohesion—conditions that can aggravate conflict dynamics and civilian vulnerability.

For the agenda, this case anchor helps delegates connect classic protection rules to modern harm pathways: even where kinetic attacks are limited, targeted disinformation, intimidation, and digitally enabled coercion can produce rights harms that fall squarely within UNHRC concern and require evidence methodologies (like the Berkeley Protocol) to support later accountability.

IX. Questions a Resolution Must Answer (QARMA)

1. Definitions and thresholds

- How should UNHRC define "hybrid warfare" for the purpose of this resolution, given that hybrid tactics may combine kinetic violence with disinformation/cyber tools and proxy relationships?
- What indicators should trigger heightened UNHRC attention to NSAG conduct: NIAC threshold, de facto territorial control, systematic detention, information control, or patterns of atrocity crimes?

2. Minimum standards for NSAG conduct

- Which customary IHL protections should be explicitly reaffirmed as binding on all parties (including NSAGs), and how should IHRL standards inform interpretation of concepts like humane treatment and indispensable judicial guarantees?
- How should the resolution address detention by NSAGs: minimum safeguards to reduce torture/ill-treatment and arbitrariness, and minimum judicial guarantees compatible with conflict realities?

3. Integration without recognition

- What compliance-raising tools can be recommended (e.g., special agreements under Common Article 3) while explicitly reaffirming that such engagement does not affect legal status?
- How should states and UN entities manage the tension between counter-terrorism frameworks and humanitarian engagement aimed at increasing respect for IHL?

4. Monitoring, reporting, and evidence standards

- Should UNHRC request that COIs/FFMs and other mechanisms systematically apply digital evidence standards aligned with the Berkeley Protocol when investigating hybrid warfare contexts?
- What minimum expectations should exist for secure evidence preservation, witness protection, and verification so NSAG violations can be prosecuted later?

5. Hybrid justice and accountability pathways

- What mix of domestic prosecutions, specialized chambers, hybrid tribunals, or universal jurisdiction cooperation should be encouraged to ensure NSAG IHL violations are penalized in practice?
- How should accountability frameworks address proxy warfare dynamics (external sponsorship and deniability) while keeping the resolution

anchored in civilian protection?

6. Victim remedies and non-recurrence

- How should the resolution connect accountability to justice and reparation, consistent with OHCHR guidance that fact-finding can recommend measures for justice and reparations and help counter impunity?
- What guarantees of non-recurrence should be emphasized for hybrid conflict environments (e.g., detention safeguards, anti-discrimination measures, restrictions on incitement/disinformation that drives violence) that align with UNDP's warnings on polarization and misinformation risks?

7. Follow-up and implementation

- What follow-up design should UNHRC adopt so recommendations do not end at "report publication" (e.g., periodic reporting by OHCHR, renewal cycles for mechanisms, implementation matrices)?

X. AGENDA 2: Addressing Human Rights Crises Amid Digital Surveillance and Impunity

SECTION I: OVERVIEW

1. Context of Digital Surveillance within Contemporary Human Rights Crises

The intersection of technology and human rights has created a new frontier for both protection and violation of fundamental freedoms. Digital surveillance, once a tool primarily used by intelligence agencies for national security purposes, has evolved into a pervasive mechanism that affects billions of people worldwide. The rapid advancement of surveillance technologies has outpaced the development of legal frameworks and oversight mechanisms, creating a dangerous gap where human rights violations can occur with alarming frequency and impunity.

In the contemporary landscape, digital surveillance encompasses a vast array of technologies and practices, from mass data collection programs that sweep up the communications of entire populations, to targeted spyware attacks that infiltrate the devices of specific individuals. These technologies can track our movements, monitor our communications, analyse our behaviour patterns, and even predict our future actions. While proponents argue that such tools are necessary for combating terrorism and crime, the reality is that they are increasingly weaponized against human rights defenders, journalists, political opponents, and vulnerable populations.

The COVID-19 pandemic accelerated the adoption of digital surveillance tools worldwide, with many governments implementing contact tracing apps, temperature monitoring systems, and digital health passes. While some of these measures served legitimate public health purposes, others created infrastructure for broader surveillance that persisted long after the emergency subsided. The pandemic demonstrated how quickly surveillance can be normalized under the guise of security or public health, and how difficult it is to roll back once implemented.

2. Intersection of Technology, Repression, and Entrenched Impunity

The marriage of advanced surveillance technology with authoritarian governance has created a new paradigm of repression. Digital surveillance enables states to monitor dissent at scale, identify opposition networks, and suppress activism before it can gain momentum. Unlike traditional forms of repression, which often leave visible evidence and can be documented by human rights organizations, digital surveillance operates in the shadows, making it difficult to detect, prove, and hold perpetrators accountable.

Impunity—the failure to bring perpetrators of human rights violations to justice—has become deeply entrenched in the digital surveillance ecosystem. This impunity operates on multiple levels. States conducting surveillance claim national security exemptions and invoke state secrets to prevent judicial oversight. Private

companies that develop and sell surveillance technologies hide behind client confidentiality and jurisdictional complexities. When abuses are exposed, the opacity of digital systems makes it nearly impossible to trace responsibility through the chain of command.

The Pegasus Project revelations in 2021 exemplified this crisis. The investigation revealed that NSO Group's Pegasus spyware had been used to target over 50,000 phone numbers, including those of heads of state, journalists, human rights defenders, and political opposition figures across at least 11 countries. Despite overwhelming evidence of abuse, NSO Group continued to operate with minimal consequences for years, protected by Israeli export controls and claims that it merely sold the technology without controlling its use. Only recently have courts begun to hold the company accountable, but the perpetrating states themselves largely remain unpunished.

3. UNHRC's Mandate and Tools in Addressing Digital-Era Violations

The United Nations Human Rights Council, established in 2006 by General Assembly Resolution 60/251, serves as the primary intergovernmental body responsible for strengthening the promotion and protection of human rights globally. The Council's mandate includes addressing situations of human rights violations and making recommendations to prevent them, promoting effective coordination of human rights within the UN system, and serving as a forum for dialogue on thematic issues.

In addressing digital-era violations, the UNHRC possesses several critical tools:

Special Procedures: The Council can appoint Special Rapporteurs or establish Working Groups to examine, monitor, and report on specific human rights situations or themes. The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has been particularly active in addressing surveillance issues, issuing reports that call for moratoriums on surveillance technology sales and advocating for stronger human rights protections.

Universal Periodic Review (UPR): This unique mechanism involves a review of the human rights records of all 193 UN Member States. The UPR provides an opportunity to highlight surveillance abuses and track whether states are implementing recommendations to address these violations.

Resolutions and Statements: The Council can adopt resolutions that condemn specific violations, call for action, or establish new mechanisms. The "Right to Privacy in the Digital Age" resolutions (A/HRC/RES/28/16, A/HRC/RES/34/7, A/HRC/RES/42/15, and subsequent resolutions) have established important norms regarding digital surveillance and privacy rights.

Complaint Procedure: This mechanism allows individuals and organizations to bring attention to consistent patterns of gross and reliably attested violations of human rights, including those related to surveillance.

Cooperation with Other Bodies: The Council works closely with treaty bodies like the Human Rights Committee (which monitors compliance with the International Covenant on Civil and Political Rights) and with the Office of the High Commissioner for Human Rights to provide technical assistance and support investigations.

4. Important Definitions

Digital Surveillance: The monitoring, collection, analysis, use, and manipulation of personal data about individuals or groups through digital technologies. This includes mass surveillance (bulk collection of data from entire populations), targeted surveillance (monitoring of specific individuals or groups), and predictive surveillance (using algorithms to anticipate behaviour or identify threats). Digital surveillance can be conducted by states, corporations, or non-state actors using tools ranging from simple data logging to sophisticated spyware capable of complete device takeover.

Impunity: The exemption from punishment or freedom from the injurious consequences of an action. In the human rights context, impunity refers to the failure to bring perpetrators of violations to justice, whether through criminal prosecution, civil proceedings, administrative sanctions, or other accountability mechanisms. Digital surveillance impunity is particularly pernicious because it involves state secrecy, corporate opacity, technical complexity, and jurisdictional challenges that collectively prevent victims from obtaining redress.

Transnational Repression: The act of governments reaching across borders to silence dissent among diaspora and exile communities. In the digital age, this includes surveillance of nationals abroad, online harassment campaigns, hacking of devices and accounts, intimidation of family members through monitored communications, and the weaponization of Interpol and extradition processes. Transnational digital repression is scalable, difficult to attribute, and creates a chilling effect that extends far beyond the immediate targets.

Spyware: Malicious software designed to infiltrate devices without the user's knowledge or consent, enabling surveillance of communications, activities, location, and data. Commercial spyware like Pegasus, Predator, and FinFisher can exploit security vulnerabilities to gain complete access to smartphones and computers. These tools can activate cameras and microphones, extract messages and emails, track location, and exfiltrate data—all while remaining undetectable to the average user.

Doxxing: The malicious disclosure of private or identifying information about an individual online without their consent, typically with the intent to harass, threaten, or intimidate. In the context of digital repression, doxxing is used to expose the identities of anonymous activists, reveal the locations of dissidents in hiding, or publish personal details to facilitate further targeting. Doxxing can have severe consequences, including physical violence, discrimination, and forced displacement.

Zero-Click Exploit: A type of cyberattack that requires no user interaction to succeed. Unlike traditional spyware that requires the target to click a link or download a file, zero-click exploits can infect devices simply through receiving a message or being connected to a network. These exploits are particularly dangerous because they eliminate the possibility of user vigilance as a defence and can target even the most security-conscious individuals.

Chilling Effect: The discouragement of legitimate exercise of rights due to fear of legal or social sanctions. In the surveillance context, the chilling effect refers to how the mere knowledge or suspicion that one is being monitored can lead to self-censorship, reduced participation in civic activities, withdrawal from online spaces, and fragmentation of social movements. The chilling effect undermines democracy by silencing dissent before it can even be articulated.

Digital Evidence: Information stored or transmitted in digital form that can be used in legal proceedings to establish facts about human rights violations. This includes metadata, communications records, geolocation data, video and audio recordings, social media content, and forensic analyses of infected devices. Digital evidence presents unique challenges related to authentication, chain of custody, technical expertise requirements, and the need to protect sources and victims from further targeting.

XI. GLOBAL IMPACT AND PREVALENCE

1. Scope of Digital Surveillance Targeting

Digital surveillance has become a universal feature of the modern landscape, affecting billions of people worldwide. However, certain populations face disproportionate targeting due to their roles in society, their identities, or their activities. Human rights defenders, journalists, lawyers, political opposition figures, minority communities, migrants, and refugees are among the most heavily surveyed groups globally.

Recent estimates suggest that approximately 80% of individuals working in civil society in high-risk environments have experienced some form of digital surveillance or online harassment. The Pegasus Project alone identified over 50,000 phone numbers as potential surveillance targets across 45 countries. In 2024, multiple investigations revealed that journalists investigating corruption, activists organizing protests, lawyers defending political prisoners, and opposition politicians challenging incumbent regimes had been systematically targeted with commercial spyware.

The scale of surveillance varies by context. In China, the government has constructed the world's most comprehensive digital surveillance state, combining facial recognition, social media monitoring, DNA collection, and predictive policing algorithms to track and control the population of 1.4 billion people. The surveillance architecture is particularly intensive in Xinjiang, where the Uyghur minority faces constant monitoring through smartphone apps, checkpoint scanning, and pervasive cameras. In less technologically advanced contexts, surveillance may be more targeted but equally devastating in its impact on specific individuals or communities.

The commercialization of surveillance technology has democratized access to powerful monitoring tools, enabling not only sophisticated intelligence agencies but also smaller states with limited technical capacity to conduct advanced surveillance. Companies like NSO Group, Cytrox, Intellexa, and dozens of others have created a global marketplace where surveillance capabilities can be purchased by any government willing to pay, regardless of its human rights record.

Impact on Civic Space, Elections, Social Movements, and Democratic Institutions

Digital surveillance has a profoundly corrosive effect on the civic space necessary for democratic societies to function. When activists know their communications are monitored, they become more cautious, sometimes to the point of inaction. Organizational meetings become fraught with suspicion about who might be recording or reporting to authorities. Coalition-building becomes difficult when potential allies fear guilt by association.

The impact on elections is particularly concerning. In multiple countries, opposition parties and candidates have been targeted with surveillance to expose campaign strategies, identify supporters, and suppress voter mobilization. In Hungary, Poland, and Spain, opposition politicians and their associates were infected with

Pegasus spyware during critical electoral periods. In Mexico, journalists investigating electoral corruption found their phones compromised. These surveillance campaigns undermine the fundamental principle of free and fair elections by giving incumbent governments an unfair advantage and deterring citizens from participating in opposition movements.

Social movements have been repeatedly decimated by surveillance-enabled repression. The 2019 Hong Kong protests saw sophisticated tracking of protesters through facial recognition, transit card analysis, and social media monitoring, leading to thousands of arrests. The 2020-2021 Thai pro-democracy protests saw activists targeted with Pegasus spyware, enabling authorities to identify organizers and predict protest actions. The 2024 Bangladesh protests that eventually led to Prime Minister Sheikh Hasina's ouster were met with extensive surveillance, internet shutdowns, and targeted arrests based on digital monitoring.

Democratic institutions themselves are weakened when surveillance becomes normalized. Judicial independence is compromised when judges know their communications can be monitored. Legislative oversight becomes hollow when parliamentarians suspect their offices are bugged. Civil service neutrality erodes when officials fear that reporting wrongdoing will result in surveillance and retaliation. Trust in government—already fragile in many contexts—further deteriorates when citizens realize the state is spying on them.

2. Psychological, Social, and Community-Level Effects

The psychological impact of surveillance on individuals cannot be overstated. Those who discover they have been targeted often experience profound feelings of violation, paranoia, and helplessness. The knowledge that intimate conversations with family, private medical information, or confidential communications with sources have been accessed by hostile actors creates lasting trauma. Many targets report anxiety, depression, insomnia, and difficulty trusting others even years after the surveillance.

Research conducted by the Citizen Lab between 2019 and 2024, involving over 80 interviews with surveillance targets in exile, revealed consistent patterns of psychological harm. Targets described constant fear that authorities might use their communications against them or their families. They reported withdrawing from activism, limiting contact with others to avoid putting them at risk, and experiencing isolation and depression. Women targets, in particular, described gender-based targeting that weaponized their private lives against them.

At the community level, surveillance fragments social cohesion. Trust within activist networks breaks down as members suspect infiltration or monitoring. Communities become risk-averse, avoiding collective action even when injustices demand response. The most vulnerable individuals—those with family members still in their country of origin, those with uncertain immigration status, or those from minorities already facing discrimination—bear the greatest burden, often forced to remain silent to protect themselves and their loved ones.

The chilling effect extends beyond direct targets. When high-profile activists or journalists are surveyed, their entire community receives the message: "You are being watched. Step out of line and you will be next." This deterrent effect is precisely what surveillance is designed to achieve. By creating an environment where everyone assumes they are monitored, surveillance becomes self-enforcing, requiring fewer resources while achieving broader compliance.

For diaspora and exile communities, surveillance creates a double displacement. Having already fled persecution in their home countries, they find themselves unable to escape the reach of the regimes they fled. They cannot safely communicate with family members back home, cannot participate in diaspora organizing without fear of retaliation against relatives, and cannot feel truly free even in countries that ostensibly protect political asylum. This psychological burden is compounded by the sense that host countries either cannot or will not protect them from digital transnational repression.

XII. ROOT CAUSES

1. Historical Evolution of Surveillance States and Security Doctrines

The roots of modern digital surveillance can be traced through decades of evolving state security practices. During the Cold War, both Western democracies and communist regimes developed extensive surveillance infrastructures to monitor perceived threats. The COINTELPRO program in the United States systematically targeted civil rights leaders, anti-war activists, and socialist organizations. The Stasi in East Germany created perhaps the most comprehensive pre-digital surveillance state, employing vast networks of informants to monitor citizens' every move.

These historical precedents established key elements that persist in digital surveillance: the expansion of "security" to encompass political dissent, the normalization of secret programs beyond public or even legislative oversight, the use of technology to scale monitoring beyond human capacity, and the criminalization of those who expose surveillance programs. The transition to digital tools amplified these tendencies exponentially.

The September 11, 2001 attacks triggered a global expansion of surveillance powers under counter-terrorism frameworks. The USA PATRIOT Act authorized unprecedented domestic surveillance, while similar legislation proliferated globally. The War on Terror created a permissive environment where civil liberties could be curtailed in the name of security with minimal accountability. Edward Snowden's 2013 revelations about NSA mass surveillance exposed how far democratic governments had pushed into warrantless monitoring of their own citizens and foreign nationals alike.

Authoritarian regimes quickly learned from Western surveillance practices while adapting them to their own contexts. China's social credit system, Russia's SORM monitoring infrastructure, and the Gulf states' extensive use of commercial spyware all reflect lessons learned from both historical surveillance states and contemporary digital capabilities.

2. Domestic Legal Frameworks Enabling Mass and Targeted Surveillance

Many countries have enacted legal frameworks that legitimize extensive surveillance powers while providing inadequate oversight or remedies. These frameworks typically share common features that enable abuse:

Vague Definitions: Terms like "national security," "terrorism," or "extremism" are defined so broadly that they can encompass peaceful dissent, journalism, or human rights advocacy. This allows governments to surveil individuals engaged in entirely legitimate activities by characterizing them as threats.

Weak Oversight: Judicial authorization requirements may be nominal, with special courts rubber-stamping surveillance requests without meaningful review. In some countries, executive branch officials can authorize surveillance without any independent oversight. Oversight bodies, where they exist, often lack the technical

expertise, resources, or independence to effectively monitor surveillance activities.

Secrecy: National security classifications shield surveillance programs from public scrutiny. Individuals targeted rarely know they are under surveillance, preventing them from challenging it. Even when courts consider surveillance cases, proceedings may be closed and evidence classified, denying defendants meaningful opportunities to contest the monitoring.

Immunity: Laws grant broad immunity to intelligence and security services, making it nearly impossible to hold them accountable for unlawful surveillance. State secrets privileges allow governments to dismiss lawsuits by claiming that disclosure of information necessary to prove abuse would compromise national security.

Data Retention: Mandatory data retention laws require telecommunications and internet service providers to store communications metadata for months or years, creating massive databases that can be searched without individualized suspicion. This infrastructure enables retrospective surveillance, where authorities can reconstruct an individual's associations and movements after identifying them as a person of interest.

Cross-Border Data Sharing: Agreements between governments enable surveillance data sharing with minimal oversight, allowing countries to circumvent their own domestic legal restrictions by obtaining information collected by foreign partners.

In Israel, for example, the export of surveillance technology like Pegasus is classified as a military export and must be approved by the Ministry of Defence. However, approval has been granted to countries with documented human rights abuses, and the Israeli government has reportedly used NSO technology sales as a diplomatic tool to strengthen relationships with other governments. This creates a system where surveillance technology becomes an instrument of foreign policy rather than being subject to human rights scrutiny.

3. Political Instrumentalization of "National Security" and Counter-Terrorism Narratives

Governments systematically weaponize security rhetoric to justify surveillance that has little to do with genuine threats. By framing dissent as extremism, journalism as espionage, and activism as terrorism, states create pretexts for monitoring anyone who challenges their authority.

The instrumentalization of counter-terrorism is particularly insidious because it exploits legitimate concerns about violence to expand surveillance powers far beyond what is necessary or proportionate. Laws ostensibly designed to prevent terrorism are then applied to environmental activists, trade unionists, indigenous rights defenders, and other groups engaged in lawful advocacy.

In Iran, human rights defenders and religious minorities are routinely accused of "endangering national security" or "espionage" for activities like documenting human rights violations or practicing their faith. In Egypt, NGO workers and journalists face terrorism charges simply for doing their jobs. In China, Uyghurs are labelled as extremists for expressing their cultural identity or practicing their religion.

This securitization of dissent has several pernicious effects. It shifts surveillance from targeted monitoring of specific threats to broad-based suspicion of entire categories of people. It stigmatizes legitimate political activity and social movements. It enables the use of extraordinary legal powers that bypass normal due process protections. And it creates a climate where courts, legislatures, and the public defer to security claims rather than demanding evidence and accountability.

4. Socio-Cultural Normalization of Monitoring and Stigmatization of Dissent

In many societies, surveillance has become so pervasive and routine that citizens accept it as an unavoidable feature of modern life. The convenience of digital services—social media, navigation apps, online shopping—comes with the price of constant data collection, conditioning people to trade privacy for functionality.

This commercial surveillance creates infrastructure and norms that governments exploit. When people are already accustomed to platforms tracking their location, analysing their communications, and predicting their behaviour for advertising purposes, government surveillance seems less exceptional. The line between commercial and state surveillance often blurs, as governments purchase data from brokers, subpoena records from companies, or co-opt platforms for monitoring.

Educational systems in some countries actively promote surveillance. Textbooks and curricula depict monitoring as protective rather than intrusive, teach children to report on each other, and normalize the presence of cameras and tracking technologies in schools. This childhood conditioning shapes adults who are less likely to question or resist surveillance.

Media representations also matter. When news coverage consistently frames surveillance as necessary for safety, depicts targets of surveillance as dangerous, and portrays those who raise privacy concerns as naive or having something to hide, it reinforces pro-surveillance attitudes. State media in authoritarian contexts explicitly promotes surveillance as patriotic and opposition as treasonous.

Social stigma against dissent reinforces surveillance's chilling effect. In societies where conformity is valued and challenging authority is seen as disrespectful or dangerous, the knowledge that surveillance identifies non-conformists creates powerful pressure to self-censor. This is especially true in collective cultures were bringing negative attention to one's family or community through surveillance has profound social consequences.

5. Power Asymmetries Between States, Individuals, and Private Tech Actors

The digital surveillance ecosystem is characterized by profound power imbalances that make accountability extremely difficult. States possess massive resources, legal authority, and technical capacity that individuals cannot match. When an intelligence agency targets someone with sophisticated spyware, the target often has no way to detect it, no means to prevent it, and no realistic path to justice even if they discover it.

Private surveillance companies occupy a unique position in this power structure. Companies like NSO Group, Cytrox, and Intellexa operate globally, selling capabilities to multiple governments while maintaining that they bear no responsibility for how their products are used. This business model deliberately obscures accountability by creating multiple layers of separation between the technology developer, the government client, and the actual abuse.

These companies benefit from regulatory arbitrage, locating headquarters, development, and sales in different jurisdictions to minimize oversight. They exploit gaps in export controls, which focus on traditional weapons while struggling to keep pace with cyber-capabilities. They hide behind non-disclosure agreements, intellectual property protections, and claims of proprietary secrets to avoid transparency about their operations.

The power asymmetry extends to evidence and proof. Victims of surveillance must overcome enormous technical and legal hurdles to demonstrate they were targeted. Forensic analysis requires specialized expertise that most individuals lack. Even when infection is confirmed, attributing it to a specific actor is challenging. Legal proceedings demand evidence that is often classified or located in foreign jurisdictions beyond the victim's reach.

Meanwhile, the surveillance industry grows increasingly sophisticated and interconnected. A global ecosystem has emerged featuring vulnerability researchers who discover exploits, brokers who buy and sell them, integrators who package them into weapons, vendors who market them to governments, and operators who deploy them against targets. Each actor in this chain claims limited responsibility while collectively enabling massive human rights violations.

Tech giants like Apple, Google, and Meta also occupy ambiguous positions. While they invest in security to protect users and occasionally sue spyware vendors, they also design platforms that collect vast amounts of data, resist end-to-end encryption in some contexts, and comply with government data requests. Their business models depend on data extraction that creates vulnerabilities surveillance companies exploit.

XIII.: VULNERABLE POPULATIONS

1. Human Rights Defenders, Journalists, Whistleblowers

Human rights defenders who document abuses, journalists who report on government corruption, and whistleblowers who expose wrongdoing are primary targets of digital surveillance precisely because their work threatens entrenched power. The targeting of these individuals serves multiple purposes: gathering intelligence about their sources and networks, obtaining advance warning of upcoming publications or campaigns, intimidating them into silence, and discrediting them by exposing private information.

The impacts on these populations are severe. Human Rights Watch staff member Lama Fakih was targeted with Pegasus spyware five times between April and August 2021, compromising her communications with crisis zones from Syria to Myanmar. Moroccan journalist Omar Radi's phone was infected with spyware while he was investigating corruption and security service abuses. Mexican journalists investigating cartel violence and government collusion found their devices compromised repeatedly.

For journalists, surveillance undermines source protection—the cornerstone of investigative reporting. When journalists know their communications are monitored, sources become unwilling to talk, severing the flow of information that exposes wrongdoing. The chilling effect extends to entire newsrooms, as editors become risk-averse and reporters self-censor to avoid putting sources in danger.

Whistleblowers face particular vulnerability because their identities must often be kept confidential for their own safety. Surveillance that unmasks a whistleblower can lead to their prosecution, job loss, physical danger, and stigmatization. The fear of surveillance deters potential whistleblowers from coming forward, allowing abuses to continue unreported.

Legal protections for these groups are often inadequate. While many countries have press freedom laws and whistleblower protection statutes, these rarely address digital surveillance threats. Even in countries with strong protections, national security exceptions can override them. Journalists covering sensitive topics like military operations, intelligence services, or government surveillance itself find that the very subjects they report on are those most aggressively monitoring them.

2. Political Opponents, Protest Organizers, Diaspora Communities

Political opposition figures and protest organizers face surveillance designed to undermine their effectiveness and deter others from joining them. In Poland, opposition leader and senator Krzysztof Brejza was hacked with Pegasus spyware during the 2019 parliamentary election campaign, with messages extracted from his phone and leaked to pro-government media in manipulated form to damage

his party. In Hungary, opposition politician Szabolcs Panyi and several other journalists and politicians were targeted with the same spyware.

Protest organizers face systematic surveillance to map networks, predict actions, and enable pre-emptive arrests. During Thailand's 2020-2021 pro-democracy protests, at least 30 activists had their phones infected with Pegasus. In Bangladesh, surveillance and internet shutdowns preceded mass arrests during the 2024 student protests. In Hong Kong, protest leaders were tracked through transit records, facial recognition, and social media analysis, leading to charges under national security laws.

Diaspora communities face the particular challenge of transnational repression, where surveillance extends across borders to reach dissidents in exile. The Chinese government monitors overseas students, activists, and academics through sophisticated combinations of social media surveillance, infiltration of diaspora organizations, pressure on family members in China, and hacking. Saudi Arabian dissidents like Omar Abdulaziz, a Canadian resident, had his phone hacked with Pegasus in the months before journalist Jamal Khashoggi was murdered—Khashoggi and Abdulaziz had been collaborating on initiatives to counter Saudi government narratives on social media.

Iranian, Rwandan, Turkish, Egyptian, and numerous other diaspora communities report systematic surveillance and harassment. The knowledge that home country intelligence services are monitoring their activities abroad creates a climate of fear even in countries that ostensibly offer asylum. Many diaspora members avoid political activity entirely to protect themselves and their families, enabling repressive regimes to silence dissent even beyond their borders.

3. Religious, Ethnic, and Racial Minorities

Minority communities face surveillance that combines discriminatory targeting based on identity with pretexts of security concern. The most documented example is China's surveillance of Uyghurs and other Turkic Muslim minorities in Xinjiang. The government has constructed what experts call a "digital prison," combining facial recognition cameras, mandatory smartphone apps that monitor all communications and activities, checkpoints that scan phones and biometric data, and predictive policing systems that flag "suspicious" behaviours.

This surveillance enables mass detention—over one million Uyghurs and other minorities have been held in "re-education camps" based partly on data from surveillance systems. The targeting extends globally, with Uyghurs abroad reporting attempts to install spyware on their devices, harassment to coerce them into becoming informants, and pressure on family members in Xinjiang to compel their return.

Muslim communities in many countries face disproportionate surveillance under counter-terrorism frameworks. In the United States, the NYPD's monitoring of Muslim neighbourhoods and mosques persisted for years. In the UK, the Prevent program's referrals show systematic bias against Muslim youth. In India, Muslim

activists and journalists documenting anti-Muslim violence have been targeted with Pegasus spyware.

Jewish communities also face targeting in various contexts. In Yemen, the tiny remaining Jewish community has been surveilled and harassed by Houthi forces. In Europe and North America, Jewish activists who criticize Israeli government policies report being labelled as "self-hating Jews" or "existential threats" and subjected to surveillance and doxxing campaigns.

Roma communities in Europe face discriminatory surveillance through welfare monitoring systems, predictive policing programs, and settlement monitoring—often justified by stereotypes of criminality. Indigenous communities worldwide report surveillance when defending land rights or opposing resource extraction projects, with their activities framed as economic security threats.

4. Women, LGBTQ+ Persons, and Gender-Based Targeting Online and Offline

Surveillance is frequently weaponized along gender lines, with women and LGBTQ+ individuals facing targeting that exploits and exacerbates existing discrimination. In Iran, women protesting compulsory hijab laws during the "Woman, Life, Freedom" movement faced intensive surveillance, with authorities using facial recognition to identify protesters, monitoring social media for "immoral" content, and pressuring families to control female members.

Gender-based digital transnational repression takes specific forms including stalking by abusive partners or family members enabled by spyware, non-consensual disclosure of sexual orientation or gender identity, threats of exposing private photographs or conversations, doxxing of women activists that includes their home addresses, and surveillance that focuses on romantic or family relationships to find leverage points.

Research by the Citizen Lab on gender-based digital transnational repression found that women target experience unique harms. They face threats of sexual violence based on surveillance-gathered information. They are doxed in ways that emphasize their gender, with attackers publishing information like home addresses or children's school locations to heighten fear. Their advocacy is delegitimized through gendered attacks that frame them as morally transgressive rather than politically threatening.

In Egypt, LGBTQ+ individuals have been entrapped through dating apps like Grindr, with police creating fake profiles to identify and locate users. Metadata from these apps has been used as evidence in prosecutions. In several countries, surveillance has exposed LGBTQ+ individuals to families or communities where they face severe consequences, including honour violence.

The intersection of gender and surveillance creates particular vulnerabilities for women journalists, women human rights defenders, and women politicians. They face both professional targeting for their work and personal targeting through gender-based attacks. Princess Latifa of Dubai and Princess Haya were surveilled with Pegasus spyware by Dubai's ruler in contexts of family disputes,

demonstrating how surveillance tools marketed for security purposes are used in intimate violence.

5. Refugees, Migrants, and Displaced Persons Monitored Across Borders

Refugees and migrants face multilayered surveillance at every stage of their journeys. Origin countries may surveil diaspora communities, as previously discussed. Transit countries often monitor refugee camps and migration routes. Destination countries subject asylum seekers to intensive data collection that can later be used against them.

The digitization of border control has created new vulnerabilities. Biometric data collection at borders, mandatory phone searches, social media screening for visa applications, and data sharing between countries all create surveillance infrastructure that refugees cannot avoid. This data can be shared with origin countries, used to deny asylum claims, or exploited by smugglers and traffickers who intercept communications.

Syrian Christian and Yazidi refugees in Lebanon and Jordan report facing discrimination in accessing services based on their religious identity, with monitoring creating barriers to aid and heightened vulnerability. Rohingya refugees in Bangladesh and surrounding countries face surveillance that restricts their movement and labour. Palestinian refugees face Israeli surveillance systems that monitor their communications and movement even in displaced settings.

Migrant workers in Gulf countries are subject to kafala sponsorship systems that give employers enormous power, often including control over workers' communications and movement through mandatory apps and SIM card restrictions. These workers, many from South Asian countries, face confiscation of devices, forced installation of tracking apps, and monitoring of all communications—a form of digital servitude that intersects with exploitative labour conditions.

Unaccompanied minors in refugee situations are particularly vulnerable. Their personal information may be collected without proper consent or safeguards, used in ways that increase rather than mitigate their risks, and shared with parties that may not have their best interests in mind. Children separated from families may have no advocate ensuring their digital rights are protected.

XIV. WARTIME AND PEACE: DIGITAL SURVEILLANCE AND IMPUNITY

1. Use of Digital Surveillance in Armed Conflict

Digital surveillance in armed conflict contexts presents unique challenges that intersect International Humanitarian Law (IHL) and International Human Rights Law (IHRL). In warfare, surveillance technologies are deployed for tactical purposes including targeting combatants, gathering intelligence, and protecting military assets. However, these same technologies create significant risks for civilians, humanitarian workers, and the distinction between combatants and non-combatants that IHL demands.

Modern conflicts increasingly blur the line between traditional warfare and digital operations. In Israel-Palestine, Israeli authorities have deployed extensive surveillance systems including biometric databases, facial recognition checkpoints, smartphone data collection, and monitoring of communications throughout occupied territories. According to recent reports, the surveillance infrastructure enables constant monitoring of Palestinian movement, restricts freedom of assembly, and facilitates arrests based on social media activity. While framed as security measures, these systems affect entire civilian populations rather than specific military threats, raising questions about proportionality and distinction under IHL.

In Sudan, the ongoing conflict between the Sudanese Armed Forces and Rapid Support Forces has involved surveillance of civilians documenting atrocities, internet shutdowns to prevent information flow, and targeting of journalists reporting on war crimes. The breakdown of state infrastructure has created accountability gaps where surveillance abuses occur without possibility of redress, while humanitarian organizations struggle to operate knowing their communications may be monitored by parties to the conflict.

Syrian conflict zones have seen the use of digital surveillance by multiple parties. The Assad government monitored opposition communications to identify rebels and activists. ISIS used captured databases and monitoring to target minorities and enforce control. Even in the post-conflict phase, surveillance of returning displaced persons creates barriers to safe repatriation and continues to victimize populations already traumatized by war.

2. Obligations of States and Parties to Conflict

Under IHL, parties to armed conflict must observe principles of distinction (differentiating between combatants and civilians), proportionality (ensuring military advantage outweighs civilian harm), and precaution (taking all feasible measures to minimize civilian casualties). These principles apply to digital surveillance tools used in conflict.

The principle of distinction is violated when surveillance systems cannot or do not differentiate between legitimate military targets and civilians. Mass surveillance of

entire populations in conflict zones, such as universal biometric collection or blanket communication monitoring, fails this test. Even when systems claim to identify combatants, algorithmic bias and technical errors create risks of misidentification with lethal consequences.

Proportionality requires that even when surveillance targets legitimate military objectives, the civilian harm it causes must not be excessive. Surveillance that exposes humanitarian workers, journalists, or medical personnel to targeting violates this principle. The use of surveillance data to construct "kill lists" or target individuals in their homes where family members may be present raises serious proportionality concerns.

Precautionary measures require parties to do everything feasible to verify targets are military objectives, choose means and methods that minimize civilian harm, and give effective advance warning of attacks. Surveillance should enhance rather than undermine these obligations. However, in practice, reliance on surveillance can create false confidence in targeting decisions, leading to strikes on civilians misidentified as combatants.

IHRL continues to apply during armed conflict alongside IHL. States cannot suspend all human rights obligations simply because hostilities exist. The right to privacy, freedom of expression, and protection from arbitrary detention persist even in war, though may be subject to greater restrictions if these are necessary, proportionate, and non-discriminatory.

3. Surveillance of Humanitarian Actors and Protection Concerns

Humanitarian organizations, medical personnel, and human rights monitors in conflict zones face particular surveillance vulnerabilities. Their communications may reveal locations of displaced persons, identities of victims providing testimony, movements of humanitarian convoys, or medical treatment of wounded combatants. When this information falls into the hands of parties to conflict, it can lead to attacks on civilians, identification of witnesses for retaliation, or targeting of humanitarian assets.

The principle of humanitarian access requires parties to conflict to allow and facilitate rapid and unimpeded passage of relief. Surveillance that monitors humanitarian communications, requires disclosure of beneficiary lists, or tracks humanitarian workers' movements can undermine this access by making it impossible to maintain neutrality and confidentiality. Organizations may be unable to reach populations in greatest need if doing so means exposing those populations to surveillance and subsequent targeting.

Medical neutrality—the principle that healthcare workers and facilities must be protected and must treat all wounded regardless of which side they fought for—is compromised by surveillance. If authorities monitor hospitals to identify wounded opposition fighters, medical facilities become targets rather than protected spaces. If healthcare workers' communications are surveilled to find patients, the fundamental trust necessary for people to seek treatment erodes.

Journalists in conflict zones face surveillance designed to prevent reporting on violations. Syrian journalists under both regime and opposition control faced monitoring and detention. Ukrainian journalists reporting on the Russian invasion found their devices targeted. Gaza journalists documenting the conflict face surveillance from multiple parties, with their communications potentially used to target sources or identify their locations.

4. Peacetime Surveillance Practices and States of Emergency

Surveillance expands during conflict or states of emergency rarely contracts when the crisis ends. Infrastructure built for counter-terrorism becomes permanent. Powers granted as temporary exceptions become normalized. Personnel trained in intrusive monitoring continue these practices even when the original justification has passed.

The COVID-19 pandemic demonstrated this phenomenon globally. Contact tracing apps, health surveillance databases, quarantine enforcement systems, and border monitoring expanded rapidly under public health emergency powers. Many of these systems persisted beyond the acute phase, repurposed for other forms of monitoring. The infrastructure and normalization created by pandemic surveillance accelerated pre-existing trends toward surveillance states.

Counter-terrorism operations provide another example. Authorities in numerous countries continue using terrorism-related legal powers for ordinary criminal investigations or even political surveillance years after specific terrorist threats have diminished. The USA PATRIOT Act's surveillance provisions, initially sold as temporary emergency measures post-9/11, were routinely renewed and expanded for decades. Similar patterns exist globally wherever counter-terrorism has been invoked to justify surveillance expansion.

States of emergency and exceptions become permanent conditions in some contexts. Egypt has been under emergency law for most of its modern history, with brief interruptions. The exceptional powers this enables, including surveillance without judicial authorization, have become ordinary tools of governance. Turkey's post-2016 coup attempt state of emergency lasted years and normalized extensive surveillance of opposition.

5. Impunity for Wartime Abuses and Peacetime Normalization

Impunity for surveillance abuses during conflict creates precedents that extend into peacetime. When parties to conflict are not held accountable for unlawful surveillance, monitoring of civilians, or misuse of surveillance to facilitate violence, these practices become templates for peacetime governance.

Iraq provides a clear example. ISIS's use of surveillance and data from captured government databases to target minorities and government employees led to mass atrocities. Yet the systematic nature of this surveillance-enabled violence has received insufficient attention in accountability processes focused more on

direct physical violence. Similarly, government surveillance that preceded ISIS's rise and facilitated sectarian violence remains unexamined.

In Colombia, decades of armed conflict involved extensive surveillance by multiple parties. Despite the peace process, surveillance practices continue, with human rights defenders and former FARC combatants reporting ongoing monitoring. The Inter-American Court of Human Rights found Colombia responsible for human rights violations through secretive and unlawful intelligence activities against lawyers and activists, establishing important precedent but having limited practical impact on dismantling surveillance infrastructure.

The normalization of wartime surveillance is particularly concerning because conflict creates permissive environments where abuses that would shock peacetime public consciousness become accepted. Once populations have experienced intensive surveillance as a survival reality in war, authorities can maintain it with less resistance in peace by invoking residual security concerns.

6. Accountability Gaps: Evidentiary Challenges, Secrecy, and Security Exemptions

Accountability for surveillance abuses in conflict is severely hampered by multiple obstacles. Evidentiary challenges include the destruction of surveillance infrastructure and records during conflict, the classification of surveillance-related documents under national security exceptions, the technical complexity of proving digital surveillance occurred, and the difficulty of attributing surveillance to specific parties when multiple actors operate in the same territory.

Secrecy doctrines invoked by states make it nearly impossible to investigate surveillance abuses. Even when victims have evidence of targeting, authorities claim that confirming or denying surveillance would compromise intelligence methods. Courts often defer to these claims rather than requiring states to provide evidence that surveillance was lawful.

Security exemptions in international cooperation frameworks create jurisdictional gaps. States refuse to extradite intelligence officials accused of unlawful surveillance, invoking national security interests. Information sharing agreements exclude surveillance-related data from mutual legal assistance. International tribunals lack jurisdiction over surveillance practices, focusing instead on physical violence and traditional war crimes.

The International Criminal Court's mandate includes crimes against humanity and war crimes, but its jurisprudence on surveillance-enabled atrocities remains underdeveloped. While persecution based on identity is recognized as a crime against humanity, the role of surveillance systems in facilitating such persecution has not been adequately examined. The ICC's 2024 policy on cyber-enabled crimes represents progress, but implementation remains uncertain.

XV. IMPUNITY MECHANISMS

1. Structural and Legal Obstacles to Accountability

Impunity for digital surveillance violations is sustained by multiple structural barriers that operate at local, national, and international levels. At the foundation, the technical complexity of surveillance creates an expertise gap. Judges, legislators, and oversight bodies often lack the knowledge to understand how surveillance systems work, making it difficult to assess whether practices comply with legal standards or to detect violations. This technical asymmetry Favors surveillance operators who can make claims that sound plausible but are misleading or false, knowing that oversight bodies cannot effectively challenge them.

Legal frameworks themselves often provide cover for surveillance impunity. Many countries have laws that explicitly immunize intelligence and security services from liability for actions taken in the course of their duties. These immunity provisions are typically broad, covering not just good-faith mistakes but also intentional violations. Even where immunity is not absolute, qualified immunity doctrines require victims to overcome high burdens to pursue accountability.

State secrets privileges allow governments to dismiss lawsuits or block investigations by claiming that allowing them to proceed would reveal classified information. This creates a catch-22: victims must prove unlawful surveillance occurred, but the evidence they need is classified, so seeking it is characterized as threatening national security. Courts routinely defer to government assertions of secrecy rather than requiring in camera review of whether classification is justified.

Secrecy laws criminalize whistleblowing and unauthorized disclosure even of illegal surveillance. Edward Snowden, who exposed massive unlawful surveillance by the NSA, faces prosecution rather than protection. Reality Winner, who leaked a document about Russian election interference, was imprisoned. Daniel Hale, who exposed civilian deaths in drone strike programs relying on surveillance, was incarcerated. These prosecutions send a clear message: exposing surveillance abuses will destroy your life even if the abuses themselves were illegal.

Standing requirements in many legal systems prevent challenges to surveillance. Courts may rule that plaintiffs cannot prove they were specifically surveilled, so lack standing to challenge surveillance programs. This is particularly absurd for mass surveillance, where the entire point is that targets don't know they're monitored. The logic creates impunity by design: if you can prove you were surveilled, the harm has already occurred; if you can't prove it, you can't challenge it.

2. Failures of Domestic Judiciaries

Even where legal mechanisms exist to challenge surveillance, domestic courts often fail to provide effective remedies. Judicial independence is compromised in many countries, with judges reluctant to rule against security services due to

career concerns, political pressure, or genuine fear. In authoritarian contexts, courts function as arms of the state rather than independent arbiters, rubber-stamping surveillance requests and dismissing challenges.

The Foreign Intelligence Surveillance Court in the United States exemplifies the problem even in democratic contexts. Of the tens of thousands of surveillance applications submitted, the court rejects a vanishingly small fraction. Proceedings are secret, targets are not represented, and decisions are not published. This creates accountability theatre rather than meaningful oversight.

Security courts in countries like Egypt, Turkey, and Pakistan have expansive jurisdiction over surveillance-related cases. These specialized tribunals lack independence, use classified evidence defence attorneys cannot access, and rarely rule against security services. Their existence channels surveillance accountability claims into forums designed to deny them.

Even well-intentioned courts face obstacles. In cases involving surveillance technology, courts may lack technical expertise to evaluate evidence. Forensic analysis showing spyware infection is technically complex and expensive, beyond the resources of most litigants. Companies like NSO Group employ sophisticated legal teams and procedural tactics to drag out cases, exhaust plaintiffs, and avoid substantive rulings.

Remedies, when granted, are often inadequate. Monetary damages don't undo surveillance violations or prevent future abuse. Injunctions may be so narrowly tailored they're easily circumvented. Criminal accountability for surveillance violations is almost non-existent—even when unlawful surveillance is proven, prosecutors rarely charge security officials, and convictions are vanishingly rare.

3. Limited Enforcement of International Norms

While international human rights law clearly prohibits arbitrary surveillance and protects privacy, freedom of expression, and other rights violated by surveillance, enforcement mechanisms are weak. The UN Human Rights Committee can issue findings and recommendations about states' ICCPR violations, but cannot compel compliance. Countries routinely ignore Committee decisions, knowing there are no consequences.

Regional human rights courts provide stronger mechanisms in theory. The European Court of Human Rights has issued important judgments on surveillance, including the 2024 Podchasov v. Russia decision that found backdoor decryption requirements violate the right to privacy. However, implementation depends on states' willingness to comply. Russia's failure to implement ECHR judgments and eventual withdrawal from the Council of Europe demonstrates the limits of regional systems when states reject their authority.

The Inter-American Court's finding that Colombia violated human rights through unlawful surveillance of human rights defenders represents significant jurisprudence but has had limited practical impact. The African and Arab regional

human rights systems have been less active on surveillance, partly due to resource constraints and partly due to political considerations.

Universal jurisdiction—the principle that some crimes are so serious any country can prosecute them regardless of where they occurred—has not been effectively applied to surveillance violations. While universal jurisdiction has been invoked for torture, genocide, and other international crimes, no country has seriously attempted to prosecute foreign officials for surveillance abuses against human rights defenders, even when those defenders have connections to the prosecuting country.

Extradition treaties typically include exceptions for political offenses or national security matters, allowing states to refuse cooperation in surveillance cases. Countries shelter their intelligence officials from foreign prosecution, invoking sovereignty and security concerns. This creates safe harbours where surveillance abusers can operate without fear of accountability.

4. Corporate Opacity and Lack of Binding Regulation

The private surveillance industry operates with remarkable opacity and minimal oversight. Companies like NSO Group, Cytrox, Intellexa, and dozens of others sell powerful surveillance capabilities to governments worldwide, yet face almost no binding regulation requiring them to respect human rights.

The UN Guiding Principles on Business and Human Rights establish that companies must respect human rights and conduct due diligence to identify and mitigate risks. However, these are voluntary guidelines rather than binding law. Surveillance companies routinely claim they conduct due diligence, but refuse to disclose their processes or criteria. NSO Group has never published its methodology for vetting clients or assessing human rights risks, despite repeated demands from civil society.

Even when abuse is documented, corporate accountability is elusive. NSO faced years of lawsuits, investigative journalism, and civil society pressure before finally experiencing significant consequences. The company was blacklisted by the US government in 2021, yet continued operating until financial troubles (related to the controversies but also to broader market conditions) led to restructuring. Criminal liability for company executives remains almost non-existent—no NSO official has been criminally prosecuted for the role their technology played in human rights violations.

Export controls ostensibly regulate surveillance technology transfers, but are poorly enforced and easily circumvented. The Wassenaar Arrangement includes some surveillance tools in its control lists, but implementation varies widely among member states. Companies exploit loopholes by routing sales through subsidiaries in less-regulated jurisdictions, claiming their technology doesn't meet technical definitions triggering controls, or arguing their products don't qualify as "weapons" even when they're as dangerous as physical arms.

Corporate structures shield surveillance companies from accountability. Complex ownership arrangements, shell companies, and jurisdictional fragmentation make it difficult to identify who truly controls these businesses and where assets are located. When one surveillance company faces consequences, its executives often simply rebrand and launch new ventures. NSO's founders have been involved in multiple surveillance companies over the years; if NSO disappears, they will likely create successors.

Non-disclosure agreements and proprietary secrecy allow surveillance companies to refuse transparency about their operations. They won't disclose client lists (though some have been revealed through litigation), won't provide details about how their technology works, and won't document the human rights impacts of their products. This opacity makes it nearly impossible to comprehensively assess the industry's harms or regulate it effectively.

XVI.: ACCESS TO JUSTICE IN THE DIGITAL AGE

1. Challenges of Documenting and Authenticating Digital Evidence

Digital evidence of surveillance violations presents unique challenges that create barriers to justice. Unlike physical evidence that can be photographed and preserved, digital evidence requires specialized forensic analysis that most victims cannot access. Confirming that a device was infected with spyware demands technical expertise, specialized tools, and time—resources typically available only to organizations like Amnesty International's Security Lab, Citizen Lab, and a handful of other research groups.

The transient nature of digital evidence compounds the problem. Surveillance leaves traces in system logs, network traffic, and file metadata, but these traces can be overwritten, deleted, or corrupted. Victims often don't realize they've been surveilled until long after the evidence has been lost. Even when evidence is preserved, proving its authenticity requires establishing a chain of custody and demonstrating that it hasn't been tampered with—difficult tasks when evidence is digital and intangible.

Attribution—determining who conducted surveillance—is particularly challenging. Forensic analysis may reveal that a device was infected with Pegasus spyware, but connecting that infection to a specific government requires additional evidence like infrastructure analysis, timing of attacks correlated with the victim's activities, or leaked documents. NSO Group and similar companies deliberately design their systems to obscure attribution, using infrastructure in third countries and anonymization techniques.

Courts often struggle to evaluate digital evidence. Judges trained in traditional law may lack the technical background to assess expert testimony about surveillance. Digital forensics is a specialized field; determining whether expert witnesses are credible and their conclusions sound requires technical knowledge judges may not possess. This creates opportunities for governments to contest evidence by presenting counter-experts who muddy the waters.

The cost of forensic analysis creates economic barriers to justice. Detailed examination of a device for spyware infection can cost thousands of dollars. Most surveillance victims cannot afford this, and legal aid rarely covers it. Some civil society organizations provide free forensic analysis, but their capacity is limited compared to the scale of surveillance globally.

2. Encryption, Anonymity, Privacy vs. Evidentiary Needs and Due Process

A fundamental tension exists between privacy-protecting technologies and accountability mechanisms. Encryption protects communications from surveillance, but also makes it difficult to obtain evidence when investigating surveillance abuses. Anonymity tools like Tor help activists evade monitoring, but can also shield perpetrators from identification.

This tension is exploited by those seeking to undermine privacy protections. Governments argue that strong encryption enables criminals and terrorists to "go dark," demanding backdoors or key escrow systems that would allow access to encrypted communications. However, the 2024 European Court of Human Rights Podchasov v. Russia judgment firmly rejected this argument, finding that requirements to decrypt communications are incompatible with human rights because they would undermine security for everyone.

The "going dark" argument is largely false in the surveillance context. Most surveillance relies on endpoint compromise (hacking devices before encryption or after decryption) rather than breaking encryption itself. NSO Group's success comes not from cracking encryption but from exploiting device vulnerabilities. Weakening encryption would thus have little impact on surveillance capabilities while significantly harming privacy and security for everyone.

From a due process perspective, the problem is not encryption but rather secret surveillance that targets defence attorneys, journalists, and witnesses in ways that undermine fair trial rights. When a defence lawyer's communications with their client are surveilled, attorney-client privilege is violated. When witnesses are monitored, they may be intimidated into silence. When judges' deliberations are compromised, judicial independence is destroyed.

Anonymity poses different challenges. Victims of surveillance may need anonymity to safely pursue justice without facing retaliation. Whistleblowers revealing surveillance programs require protection. Yet anonymity can also be abused by those conducting surveillance to evade responsibility. The solution is not to eliminate anonymity, but rather to ensure that accountability mechanisms don't depend solely on identifying individuals when institutional responsibility can be established.

3. Protection of Victims, Witnesses, and Digital Security of Legal Practitioners

Pursuing justice for surveillance violations creates risks that must be managed. Victims who come forward publicly may face intensified surveillance, retaliation against family members, prosecution on fabricated charges, or stigmatization in their communities. Witness protection systems designed for traditional crimes are inadequate for digital threats—relocating someone doesn't protect them from continued surveillance of their communications.

Legal practitioners defending surveillance victims face targeting themselves. Lawyers representing dissidents, human rights organizations providing legal services, and paralegals handling sensitive cases all become surveillance targets. Their communications with clients may be monitored to obtain privileged information. Their research and case strategy can be compromised. In extreme cases, lawyers themselves face prosecution, disbarment, or violence.

Digital security becomes essential for legal practice in surveillance contexts, yet most lawyers lack training in operational security. Secure communications require using encrypted messaging apps, but also understanding metadata,

authentication, and protection against endpoint compromise. Document security demands more than password-protecting files; it requires secure storage, careful handling of devices, and awareness of forensic traces.

The digital security burden falls disproportionately on victims and their advocates rather than on perpetrators who have state resources. This asymmetry means that even when victims want to pursue justice, the risk-benefit calculus may not favour doing so. If coming forward means exposing oneself and one's family to greater danger without reasonable prospects of accountability, many rationally choose silence.

Protection mechanisms must therefore extend beyond physical security to digital security. This includes: providing secure communications infrastructure for victims and lawyers; offering digital forensics and security training; establishing funds to cover costs of security tools and services; creating secure whistleblower channels for reporting surveillance abuses; and ensuring that engagement with justice mechanisms doesn't require victims to expose themselves to greater surveillance risk.

4. Role of International Mechanisms

Given the failures of domestic accountability for surveillance, international mechanisms become crucial. UN Special Procedures, particularly the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, have been among the most active voices calling out surveillance abuses and advocating for accountability. These mandates can document violations, pressure states through public reporting, and contribute to norm development even when they cannot directly enforce compliance.

The Universal Periodic Review process provides another avenue. Civil society organizations regularly submit information about surveillance violations for consideration in UPR reviews, and recommendations to address these violations are made to states. While states can reject recommendations, the public record of what was recommended and refused creates political pressure and documentation for future accountability efforts.

Regional human rights courts and commissions provide stronger mechanisms where they exist and states are subject to their jurisdiction. The European Court of Human Rights' surveillance jurisprudence is well-developed, establishing important precedents about necessity, proportionality, and adequate safeguards. The Inter-American Court has begun developing similar jurisprudence, as seen in its Colombia ruling. However, the African and Arab systems remain less active on surveillance issues.

The International Criminal Court's potential role is still emerging. The Court's 2024 policy on cyber-enabled crimes acknowledges that technology can facilitate crimes within the Court's jurisdiction. Surveillance systems that enable crimes against humanity (such as persecution of groups) or war crimes (such as targeting of protected persons) could theoretically be examined by the Court. However, practical barriers including limited jurisdiction, challenges of attribution and

evidence, and the Court's focus on physical violence mean that ICC accountability for surveillance violations remains more theoretical than realized.

Treaty bodies like the Human Rights Committee that monitor compliance with the ICCPR can issue General Comments interpreting treaty obligations and can consider individual complaints where states have accepted optional protocols. The Committee has been active in privacy protection, issuing General Comment No. 16 on Article 17 (privacy) which, though outdated, established important principles. The Committee is currently revising this General Comment to address digital surveillance, which will provide updated authoritative interpretation of privacy rights.

International mechanisms face significant limitations. They cannot compel compliance by powerful states that reject their authority. They rely on voluntary cooperation from states for information and implementation. Their resources are limited compared to the scale of surveillance globally. Nevertheless, they play crucial roles in norm-setting, documentation, and providing forums for victims' voices even when immediate accountability is not achieved.

XVII: INTERNATIONAL AND REGIONAL LEGISLATION

1. International Covenant on Civil and Political Rights (ICCPR)

The ICCPR, adopted in 1966, provides the primary international legal framework for privacy rights and other freedoms violated by surveillance. Article 17 protects against arbitrary or unlawful interference with privacy, family, home, or correspondence. The UN Human Rights Committee has interpreted this to cover digital communications and data, establishing that mass surveillance, indiscriminate data collection, and targeted hacking can all violate Article 17.

Article 19 protects freedom of expression, including the freedom to seek, receive, and impart information through any media. Surveillance that chills free expression or targets journalists and human rights defenders violates Article 19. Article 21 protects freedom of assembly, and Article 22 protects freedom of association—both undermined by surveillance of protest movements and civil society organizations.

The Human Rights Committee's General Comment No. 16 on Article 17, though dated, established that privacy protections extend beyond physical spaces to communications and personal information. The Committee has also addressed surveillance in concluding observations on state reports and in decisions on individual complaints. The Committee is currently revising General Comment 16 to comprehensively address digital age surveillance, which will provide critical interpretive guidance.

Article 2(3) of the ICCPR requires states to provide effective remedies for violations. This means that surveillance abuses must be investigated, perpetrators held accountable, and victims provided with reparations. The structural impunity described in this guide represents systemic failure to meet Article 2(3) obligations.

2. Convention Against Torture (CAT)

The Convention Against Torture, adopted in 1984, applies to surveillance contexts where monitoring is combined with or leads to cruel, inhuman, or degrading treatment. The Committee Against Torture has recognized that surveillance can constitute psychological torture when it is systematic, involves threats or intimidation, and causes severe mental suffering.

Several applications are relevant to digital surveillance. First, when surveillance information is used to facilitate physical torture, as when communications are monitored to identify dissidents who are then arrested and tortured. Second, when the surveillance itself involves such invasive and persistent monitoring that it causes severe psychological trauma. Third, when surveillance is used to enable cruel treatment like enforced disappearance (monitoring to track targets) or sexual violence (using private information for blackmail or exposure).

Article 2 of CAT requires states to take effective measures to prevent torture, which includes ensuring that surveillance technologies are not used in ways that

facilitate torture. Article 14 requires effective remedies for torture victims, which extends to those whose surveillance-enabled treatment violated CAT.

The Committee has addressed surveillance in several contexts. In reviewing China's record, the Committee expressed concern about surveillance's role in Xinjiang's mass detention system. In examining other countries, the Committee has raised concerns about surveillance enabling enforced disappearance and about the psychological impacts of intensive monitoring.

3. UN Guiding Principles on Business and Human Rights

The UN Guiding Principles on Business and Human Rights (UNGPs), adopted in 2011, establish that businesses have a responsibility to respect human rights. This includes conducting human rights due diligence to identify, prevent, mitigate, and account for how their operations effect human rights, and providing remedies when they cause or contribute to harms.

For the surveillance industry, the UNGPs require companies to assess the human rights risks of their products, implement policies and procedures to address those risks, and provide accountability when their technology enables abuses. NSO Group and similar companies claim to follow the UNGPs but refuse to disclose their due diligence processes or provide meaningful remedies to victims.

Surveillance companies cannot satisfy UNGP obligations through mere vetting of government clients. Human rights due diligence requires ongoing monitoring of how products are actually used, meaningful investigation of reported abuses, and termination of relationships with clients misusing technology. NSO's repeated claims that they investigate abuse while providing no evidence of such investigations or consequences for abusing clients demonstrates the gap between UNGP requirements and industry practice.

The UNGPs also establish state duties to protect against business-related human rights abuses, including through effective regulation, enforcement of laws, and ensuring access to remedy. States that host surveillance companies or approve exports have duties to ensure these companies respect human rights—duties that are systemically failing.

4. Regional Human Rights Instruments

Regional human rights systems provide additional legal frameworks. In Europe, the European Convention on Human Rights Article 8 protects privacy, with extensive European Court of Human Rights jurisprudence establishing strict requirements for lawful surveillance. The Court's cases like Big Brother Watch v. UK, Zakharov v. Russia, and Centrum för Rättvisa v. Sweden have established that mass surveillance regimes violate Article 8 unless they include robust safeguards.

The EU's General Data Protection Regulation (GDPR), while primarily a data protection law, establishes principles relevant to surveillance including purpose limitation, data minimization, and accountability. The Charter of Fundamental

Rights of the European Union protects privacy (Article 7) and data protection (Article 8) as distinct rights, with the Court of Justice of the European Union interpreting these to limit surveillance practices.

In the Americas, the American Convention on Human Rights Article 11 protects privacy, with the Inter-American Court of Human Rights beginning to develop surveillance jurisprudence. The Court's 2024 CAJAR v. Colombia judgment establishing state responsibility for unlawful intelligence activities against human rights defenders is a landmark decision.

In Africa, the African Charter on Human and Peoples' Rights does not explicitly mention privacy but has been interpreted to include it. The African Commission on Human and Peoples' Rights has issued guidance on freedom of expression and access to information that addresses surveillance. However, African regional mechanisms remain underdeveloped on surveillance issues.

The Arab Charter on Human Rights includes privacy protections but has been criticized for its limitations and the weak enforcement mechanisms of the Arab human rights system. Implementation varies widely among Arab states, many of which conduct intensive surveillance.

5. Emerging Data Protection and AI Governance Frameworks

New frameworks are emerging to address data protection and artificial intelligence, with implications for surveillance. The GDPR has influenced data protection laws globally, with over 100 countries now having some form of data protection legislation. However, these laws vary significantly in scope and enforcement, and many include broad exceptions for national security that exempt surveillance.

The Council of Europe's modernized Convention 108+ (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) provides international standards for data protection. The Budapest Convention on Cybercrime addresses some surveillance-related issues including data retention and access to stored communications data.

Emerging AI governance frameworks are beginning to address surveillance technologies. The EU's AI Act includes provisions on biometric identification and categorization, with particular scrutiny of remote biometric identification in publicly accessible spaces. However, exceptions for law enforcement and national security limit the Act's applicability to government surveillance.

UNESCO's Recommendation on the Ethics of Artificial Intelligence includes principles relevant to surveillance, including proportionality, do no harm, and fairness. The UN Secretary-General's High-Level Advisory Body on Artificial Intelligence is developing recommendations that may address surveillance. However, these emerging frameworks are at early stages and their effectiveness remains to be seen.

The fundamental challenge is that surveillance technologies evolve faster than legal frameworks. By the time regulations are developed, new capabilities have emerged that circumvent them. Effective governance must therefore focus on principles and human rights obligations rather than specific technologies, must include strong enforcement mechanisms, and must address the structural issues of opacity, impunity, and power asymmetry that enable surveillance abuses.

XVIII: CASE STUDIES

Case Study 1: Saudi Arabia – Transnational Digital Repression and Targeting of Dissidents

Saudi Arabia's use of digital surveillance exemplifies transnational repression targeting dissidents abroad. The most prominent case is journalist Jamal Khashoggi, whose murder in Istanbul in October 2018 was preceded by surveillance. Saudi dissident Omar Abdulaziz, a Canadian resident, had his phone hacked with Pegasus spyware. Abdulaziz and Khashoggi had been collaborating on initiatives to counter Saudi government narratives online. The surveillance of Abdulaziz likely provided information about their work and Khashoggi's activities.

Other Saudi dissidents have been targeted with sophisticated surveillance. Women's rights activists like Loujain al-Hathloul faced monitoring before their arrests. Saudi human rights defenders abroad report persistent attempts to install spyware on their devices. The Saudi government has allegedly used multiple surveillance vendors, not just NSO Group.

The surveillance enables an online-offline continuum of repression. Digital monitoring identifies critics, tracks their networks, and gathers intelligence. This information then facilitates physical repression including arrests, enforced disappearances, and in extreme cases, assassination. Family members in Saudi Arabia are pressured or detained to coerce dissidents abroad into silence.

Obstacles to accountability are severe. Saudi Arabia has not cooperated with investigations into Khashoggi's murder or surveillance of dissidents. Officials implicated in abuses have faced no real consequences domestically. NSO Group claims it ended its Saudi contract after concerns emerged about misuse, but only after years of documented abuse and only under international pressure.

The Khashoggi case prompted some response—sanctions on individuals, congressional criticism, and temporary pause in some arms sales—but substantive accountability has not been achieved. Saudi Arabia continues to receive military support from Western governments, NSO Group's Israeli government sponsor approved sales to Saudi Arabia for years despite known abuses, and civil lawsuits seeking accountability have struggled with jurisdictional and immunity barriers.

Case Study 2: China – Systematic Digital Surveillance and Minority Populations

China has constructed the world's most comprehensive digital surveillance state, with particular intensity in Xinjiang targeting Uyghur and other Turkic Muslim minorities. The surveillance architecture includes: facial recognition cameras tracking movements; mandatory smartphone apps monitoring communications and daily activities; frequent checkpoint inspections scanning phones and collecting biometric data; predictive policing systems flagging "suspicious" behaviours; and DNA collection from entire populations.

This infrastructure enables mass detention. Over one million people have been held in "re-education camps" based partly on surveillance data identifying them as threatening. Behaviours flagged as suspicious include: refusing to use smartphones; uninstalling apps that surveil users; contacting family abroad; praying regularly; growing a beard; or deviating from approved daily routines.

The surveillance's chilling effect is profound. Uyghurs report complete self-censorship, avoiding any expression of cultural or religious identity that might be flagged. Families are separated as those deemed suspicious are detained. Economic activity is constrained as surveillance restricts movement and employment. Cultural practices are abandoned as surveillance makes their continuation too dangerous.

The system extends globally. Uyghurs abroad report Chinese authorities hacking their devices, pressuring them to return to China, and threatening family members to coerce compliance. Chinese overseas police stations have been established in numerous countries, reportedly to facilitate surveillance and pressure tactics. Chinese students abroad face monitoring through apps required to communicate with China and face consequences for overseas activism.

International responses have been limited. While some sanctions have been imposed on Chinese officials and companies involved, these have minimal impact. Technology companies continue to sell surveillance equipment to China. The UN has struggled to address the situation, with China's position as a permanent Security Council member and major economic power limiting possibilities for accountability.

Documentation of the surveillance system relies heavily on leaked documents, satellite imagery, testimony from those who escaped, and forensic analysis of mandatory apps. The Chinese government denies abuses and restricts access to Xinjiang, making comprehensive investigation difficult. The surveillance prevents internal documentation, as anyone caught documenting violations faces severe punishment.

Case Study 3: Egypt – Digital Crackdown on Civil Society and Protest Movements

Egypt's digital surveillance targets civil society organizations, journalists, and activists who participated in the 2011 revolution or subsequent protests. Social media monitoring identifies critics, with arrests following posts critical of the government. Cybercrime and terrorism laws are applied broadly to criminalize online dissent, with vague provisions allowing prosecution for "spreading false news" or "misusing social media."

The government uses surveillance to map activist networks and pre-empt mobilization. During the 2019 protests sparked by corruption allegations, authorities arrested thousands based on social media activity and surveillance. NGO workers face surveillance of their communications, with information used to justify prosecutions under foreign funding laws that criminalize receiving international support.

Journalists face particularly intensive surveillance. Those investigating corruption, documenting human rights violations, or reporting on security force abuses have been targeted. Egyptian journalist Solafa Magdy was targeted with Pegasus spyware while detained, as was her husband, activist Hossam el-Sayed. The surveillance aimed to identify sources and monitor communications with international media and human rights organizations.

Youth movements that drove the 2011 revolution have been decimated through surveillance-enabled repression. The government identified activists through social media monitoring, arrested organizers, and prosecuted them for terrorism or assembly violations. The chilling effect has been profound, with political organizing now primarily driven underground or abroad.

Legal challenges face a biased judiciary. Egyptian courts have upheld terrorism and cybercrime convictions based on flimsy evidence while dismissing challenges to surveillance practices. Lawyers defending surveillance victims have themselves been targeted, with human rights lawyers facing travel bans, asset freezes, and prosecution.

Case Study 4: Iran – Surveillance of Women's Rights Movements and Political Dissent

Iran's surveillance intensified dramatically during the "Woman, Life, Freedom" protests that erupted after Mahsa Amini's death in police custody in September 2022. Authorities used facial recognition to identify protesters, monitored social media for "immoral" content like women without hijab, and pressured families to control female members. Many women identified through surveillance faced arrests, prosecutions, and in some cases, sexual violence in detention.

Surveillance of women's rights activists predates the 2022 protests. Activists like Shaparak Shajarizadeh, who protested compulsory hijab, had her phone hacked before her arrest. Civil society groups report persistent targeting with spyware, particularly when organizing campaigns or communicating with international organizations.

Internet shutdowns and platform throttling became tools of repression during protests. Authorities throttled Instagram and WhatsApp, blocked VPNs, and shut down internet entirely in certain areas during peak protest times. These measures isolated protesters, prevented coordination, and blocked documentation of state violence.

Doxxing of activists has been systematic. Pro-government accounts publish personal information about protesters, including home addresses and family details, to facilitate harassment and violence. Women activists face gender-specific doxxing that threatens sexual violence or exposes private information in ways meant to shame them in conservative communities.

The surveillance targets activists abroad as extensively as those in Iran. Iranian diaspora members report hacking attempts, online harassment campaigns, and pressure on family members in Iran. The long arm of Iranian surveillance reaches protest organizers in Europe, North America, and across the Middle East.

Legal accountability is non-existent within Iran. Courts prosecute surveillance victims rather than perpetrators. International accountability has been similarly limited, though UN Special Procedures have documented abuses and some sanctions have been imposed on individuals and entities involved in the crackdown.

Case Study 5: Israel/Palestine – Surveillance, Occupation, and Population Control

Israeli surveillance of Palestinians operates at multiple levels, from pervasive monitoring in occupied territories to targeting of activists and journalists. The surveillance infrastructure includes biometric databases containing information on virtually all Palestinians in the West Bank; facial recognition systems at hundreds of checkpoints; monitoring of social media for "incitement"; and smartphone data collection through both overt and covert means.

This surveillance enables population control far beyond security purposes. Movement through checkpoints is tracked and can be restricted based on surveillance data. Employment in Israel requires permits that depend on security clearances based partly on surveillance. Social connections can affect one's security classification—associating with someone flagged creates risk for all their contacts.

Activists and journalists face targeted surveillance. Palestinian human rights organizations have had staff targeted with Pegasus spyware, compromising their work documenting Israeli human rights violations. Al Jazeera journalist Givara Budeiri was surveilled before being detained and assaulted by Israeli forces while reporting in Jerusalem. The surveillance chills documentation of abuses and weakens Palestinian civil society.

The legal framework is deeply contested. Israel invokes security needs under International Humanitarian Law, which allows certain surveillance during occupation. Palestinians and human rights organizations argue the surveillance far exceeds what IHL permits, violates human rights law that continues to apply during occupation, and constitutes collective punishment. The question of which legal regime applies—IHL, IHRL, or both—remains disputed.

Accountability mechanisms are severely limited. Israeli military courts that handle cases from occupied territories have conviction rates above 99% and rarely seriously examine challenges to surveillance. Israeli civil courts have limited jurisdiction over military matters. Palestinian courts lack jurisdiction over Israeli actions. International mechanisms face Israeli non-cooperation.

Recent reports have revealed Israel's use of predictive AI systems like "Lavender" and "Gospel" to select bombing targets in Gaza, relying on mass surveillance data. These systems reportedly generated thousands of potential targets with minimal human oversight, raising profound questions about proportionality, distinction, and the use of automated systems to make life-and-death decisions in warfare.

Case Study 6: Sudan – Digital Surveillance, Conflict, and Humanitarian Crises

Sudan's digital surveillance during political upheaval and armed conflict demonstrates how surveillance intersects with broader humanitarian crises. During the 2018-2019 protests that eventually led to Omar al-Bashir's ouster, security forces monitored social media, arrested activists based on online activity, and shut down internet to prevent organization. After the April 2019 Khartoum massacre, internet was cut to prevent documentation of the violence against protesters.

Following the October 2021 military coup and the April 2023 outbreak of war between the Sudanese Armed Forces (SAF) and Rapid Support Forces (RSF), surveillance became a tool of conflict. Both sides monitor communications to identify opponents, track movements of rivals, and gather intelligence. Journalists and activists documenting atrocities face targeting from whichever side they expose.

Internet shutdowns have severe humanitarian consequences. They prevent communication among displaced families, block access to information about safe routes or services, and handicap humanitarian organizations trying to coordinate aid delivery. Documentation of violations becomes nearly impossible when connectivity is cut.

Communities documenting atrocities face surveillance from multiple parties. Those recording RSF ethnic violence in Darfur risk being identified through surveillance and targeted. Those documenting SAF strikes on civilian areas face similar risks. The militarization of surveillance means no party is safe to document, creating accountability gaps.

The enduring impunity is striking. Both SAF and RSF have committed violations with no accountability. The surveillance enabling these violations operates without oversight. International mechanisms struggle to investigate in the active conflict environment, and Sudan's domestic institutions have collapsed, eliminating any possibility of local accountability.

XIX. Questions a Resolution must answer (QARMA)

- What specific surveillance and monitoring technologies are in scope (e.g., lawful intercept, spyware, biometrics/facial recognition, IMSI catchers, mass CCTV analytics, social media monitoring, data brokers), and what uses are categorically prohibited (e.g., targeting based on protected characteristics)?

- What is the minimum legality standard: which laws must exist (public, precise, accessible), what agencies may conduct surveillance, and what penalties apply for unauthorized surveillance?

- What tests of necessity and proportionality must be met for any intrusive surveillance, and how are these tests operationalized (targeting thresholds, data minimization, time limits, geographic limits)?

- What authorisation model is required for targeted surveillance (independent judicial warrant vs other), and what emergency exceptions exist—plus how quickly must emergency authorisations be reviewed and either validated or terminated?

- What safeguards address "mass" or bulk collection: under what conditions (if any) is bulk collection permitted, what narrowing mechanisms are mandatory, and how is effectiveness demonstrated without normalizing population-wide monitoring?

- What transparency obligations apply (public transparency reports, legal basis disclosure, aggregate statistics, vendor/contracts disclosure), and what secrecy claims are unacceptable because they defeat accountability?

- What rules govern private-sector involvement: procurement standards, vendor due diligence, export controls/end-use restrictions, and liability for companies enabling abuse (including cross-border supply chains and intermediaries)?

- What independent oversight architecture is mandated (parliamentary oversight, independent regulators, data protection authority powers, national human rights institutions, inspector-general style audits), and what minimum powers must oversight bodies have (access to code/procurement files, subpoena power, on-site inspections, protected reporting channels)?

- What individual rights and remedies are guaranteed: notice (where compatible with investigations), ability to challenge surveillance legality, access/correction/deletion rights, compensation, and meaningful protection

for journalists, HRDs, lawyers, opposition figures, and whistleblowers?

- What accountability pathway applies to abuses: evidence preservation, investigatory triggers, sanctions (administrative/disciplinary/criminal), chain-of-command responsibility, and international cooperation mechanisms when surveillance is transnational (mutual legal assistance, cross-border complaint handling, and safe reporting for diaspora targets)?