The Future of International Security:
Challenges for Responses to the World's Changing Security Landscape

Discussion paper with preliminary thoughts prepared for the World Economic Forum (WEF)'s Global Future Council on International Security
Dr Annette Idler, University of Oxford, November 2017

This paper outlines the actors, mechanisms, and norms that compose the current international security architecture in order to enhance understanding on anticipating, preventing, and responding to threats to the global public good 'international security'. It identifies challenges in the current system with a view to developing a strategy to transform it into a more efficient one that is 'fit-for-purpose' to address the security challenges of the 21st century.

1. Stakeholders in International Security

This paper is based on the WEF's Global Future Council's definition of 'international security' as the system of policies, norms, and multi-stakeholder collaborations that minimize the likelihood and consequences of organized violence [original wording: conflict] between states and/or non-state actors. To illustrates the variety of stakeholders relevant to the definition, below is a (non-exhaustive) list of some of the main actors directly or indirectly participating in, or responding to, organized violence.

State Actors	**Non-state Actors**
- Governments (armed forces, police, intelligence) - International Organisations (e.g. via peace operations) - Regional Organisations (e.g. African Union, European Union) - Alliances (formal) (e.g. NATO) - Coalitions (temporary) (e.g. Global Coalition against Daesh) - …	- Insurgent groups - Terrorist organisations - Paramilitaries - Organized criminals ▪ hacking groups ▪ gangs ▪ drug cartels ▪ pirates - Foreign fighters - Mercenaries - ….

In line with the definition, a stakeholder mapping of the international security system that focuses on response actors includes:

i. actors participating in, and responding to, organized violence;
ii. actors involved in strategic planning and policymaking;
iii. actors developing the evidence base and wider knowledge on settings of organized violence drawn on by other stakeholder groups.

The graph in the annex visualizes these three stakeholder groups as inner, intermediate, and outer rings related to threats to international security. The distinction between those fueling and participating in conflict and those responding to, or aiming to mitigate can be blurred and depends on perspective. In fact, these labels are often Western-biased. Locally, 'rogue states' may be perceived to provide stability; 'peacekeepers' may be perceived as illegitimate, external intervention; and 'terrorists' may be perceived as governance-providers, for example. Discussions on reforming or transforming the international security architecture currently hardly account for this divergence of perceptions.

2. Norms and Mechanisms as Responses

The norms, mechanisms, and bodies of law to maintain the common public good of international security are mostly developed in the "intermediate ring". These include:

- International Humanitarian Law, including the Geneva Conventions and Hague Conventions;
- the UN Charter as well as treaties related to specific themes, such as the Arms Trade Treaty and the Nonproliferation Treaty;
- non-binding commitments, such as Sustainable Development Goal 16;
- further norms and approaches, such as the Responsibility to Protect and the upholding of Human Security; and response mechanisms such as sanctions.

These norms and mechanisms have evolved in parallel with changes in the international system from a state-based one to a 'world paradigm system' in which non-state actors have gained relevance. This is reflected in the widening of the scope of issues addressed, for example from a focus on the regulation of international armed conflict and the protection of civilians in armed conflict, to also include issues such as preventing weapons of mass destruction from falling into the hands of terrorists.

Norms and response mechanisms account for the *existence* of a wide range of state and non-state actors who engage in organized violence and are therefore relevant to the international security system. However, they manifest shortcomings in addressing changes in their *modus operandi*. Most are shaped by state-centric approaches to assessing threats to security and to determining thresholds for when, where, and how to respond to them. Traditional conflict measures such as the number of battle deaths influence such assessments. As a result, security policies continue to react to, rather than anticipate, future changes in conflict. This concerns the international, regional, and national level. For instance, in Haiti, UN peacekeeping operations started with a civil war approach yet security dynamics on the ground were increasingly influenced by criminal violence. In Afghanistan and Iraq, international intervention followed a counterinsurgency paradigm, neglecting hybrid methods in war. In Ukraine, governments' manipulation and influence over local communities through social media was underestimated. In Colombia, the post-conflict strategy prioritizes the demobilized rebels, even though multiple violent non-state groups continue to shape the security landscape. Rather than the absence of norms, mechanisms, and policies, it is their erosion in the face of evolving security threats, which requires attention.

3. Five Challenges to the International Security Architecture

This section sketches the challenges to our responses that arise from violent non-state groups, that is, non-state actors who participate in organized violence. They concern each of five dimensions of change in conflict: actors, impact, environments, methods, and resources. Geopolitical shifts, demographic

pressures, an increasing disconnect between power centres and communities at the margins, and the emergence of new technologies drive changes in conflict that are related to security stakeholders more broadly. Geopolitical shifts for example call into question the UN Security Council's current membership, and demographic pressures require rethinking how to share responsibilities in preventing outbreaks of conflicts due to diseases or resource scarcity. In line with this year's theme for the Global Future Council Meeting in Dubai ("The Globalization of Knowledge in a Fractured World"), the focus here is on the last two trends: the disconnect between power centres and communities at the margins, and the emergence of new technologies.

i. Who (Actors): Proliferation versus Recognition of Non-state Actors

A major trend in the world's security landscape is the proliferation of violent non-state groups. According to the International Committee of the Red Cross, more new groups have formed in the past six years than in the previous six decades combined. In eastern parts of the Democratic Republic of Congo the number of violent non-state groups has been growing to more than seventy different groups; accounts of groups in Libya are moving from listing hundreds to thousands; and, according to the Carter Center, in Syria around seven thousand groups claim their presence. Across the globe, violent non-state groups have gained visibility through setting up online profiles, often inflating their power position through online tools in order to count as relevant stakeholders on the security map. The proliferation of violent non-state groups poses challenges for our responses. The International Committee of the Red Cross and the United Nations are developing thinking on understanding, analysing, and engaging groups such as gangs, militias, and other non-state armed groups, but many questions remain unanswered. What kind of groups should international organisations engage with, and if so, how? What does the proliferation of groups mean for norms related to their recognition?

ii. What (Impact): Violence versus Illicit Governance

International attention on violent non-state groups such as Daesh focuses on their violent behaviour, neglecting their ability to exercise authority and to assume governance functions including the provision of basic services and competitive illicit economic alternatives. A large variety of armed actors exert control over civilians: religiously motivated groups such as the Taliban in Afghanistan; ethnically motivated groups such as the Moro Islamic Liberation Front in the Philippines; ideologically motivated groups such as the Maoists in India; and economically motivated groups such as drug cartels in Mexico. Illicit governance, through which groups capture territory, and the challenges it brings for nation states, is nothing new and exists across the globe. Examples include state-like forms of governance where groups tax populations, issue ID cards, or set up checkpoints on roads. Yet the context in which these illicitly governed spaces emerge is changing—with a significant impact on state-society relations. Today, central power holders are rejected and perceived to be in crisis, and technology is used to promote these views across regions. Against this backdrop, violent non-state groups who provide basic services and public goods are perceived to be legitimate authorities. This erodes states from within and fragments governance across territories. How can outside interventions account for the perceptions of communities who are alienated from states to avoid an expansion of safe havens and illicit economies? How can we move from military-centred approaches to inclusive security policies?

iii. Where (Environments): Transnationality and Cyberspace

Conflict actors and other violent non-state groups are expanding their transnational operations. This poses challenges to tackling threats to security on three levels. Locally, by jeopardizing the physical security of local communities; regionally, by producing "problems without passports" such as refugee flows and security impacts arising from various forms of transnational organized crime, including drug violence; and globally, by transforming ungoverned spaces into safe havens for global terrorism. Globally operating violent non-state groups at times even challenge the entire state system rather than single governments. The spread of means of virtual communication further facilitates the transnational modus operandi of violent non-state groups. Cyberspace itself has become another conflict theatre that violent non-state groups use to consolidate their power. How can we transform current response mechanisms tailored to local, regional, and, to some extent, transnational, levels, into mechanisms that operate "glocally" by cutting across all these levels? How can international humanitarian law be made 'fit-for-purpose' for cyberspace as a non-physical space that is least integrated into our responses?

iv. How (Methods): Interconnectedness and Information Technologies

Access to emerging technologies yields changes in the methods of non-state actors participating in organized violence as well as state actors who draw on proxies or cooperate with non-state actors. This access has facilitated the establishment of networked, interconnected structures among such actors, while the international community's norms and mechanisms to respond to threats to international security remain largely in siloes. Mechanisms address actors of single categories (e.g. counterinsurgency, counter-terrorism, operations against piracy, etc.), but it is the very interconnectedness of these phenomena and the actors involved that make them so resilient. Rebels subcontract computer hackers, terrorists engage in spot sales with arms traffickers, human smugglers work together with militias, and drug cartels cooperate with paramilitaries. How can state responses that are mostly static and constrained by large bureaucracies be transformed to anticipate, rather than react to, links among various violent non-state groups who operate in quickly shifting alliances and resilient, networked structures?

Violent non-state groups can consolidate their global support through easy access to emerging technologies because it has led to an unprecedented acceleration of the spread of information across the world. They can expand their support base through recruitment via social media, which are also used to mobilize people more generally, as the Arab Spring in 2011 demonstrated. Information is manipulated to make it consistent with the messages respective stakeholders wish to communicate to their supporters or opponents. With the growing accessibility of information, marginalized communities are becoming more aware of global inequalities and deprivation. This is likely to fuel grievances in already disadvantaged regions of the world. Depending on the governance structure in place, such grievances may lead to more violent conflict. Or violent non-state groups may channel them into promoting resistance against the state by offering alternative forms of governance that are considered to bring more justice and equality than states are able to provide. How can emerging technologies be harnessed to increase the state's perceived legitimacy in such territories rather than being exploited to undermine it?

v. *By which means (Resources): Cybercrime and 3D Printing*

The income sources of conflict actors are shifting towards cyberspace. Violent non-state groups have historically engaged in illicit activities to sustain their operations. Often, they are involved in multiple forms of illicit activities simultaneously, and single conflict territories feature various types of illicit business. In Libya for example, routes for legal commerce are also used for various forms of illicit trade, including the trafficking of drugs, weapons, and humans. In Syria, antiquities smuggling is linked to weapons trafficking. Moving transactions from physical space to cyberspace opens more opportunities for both state and non-state actors to fuel conflict. Platforms to purchase and sell weapons and other goods such as the dark net are becoming more sophisticated, while law enforcement measures are lagging further behind. Furthermore, 3D printing as an alternative way to 'purchase' weapons or drones is likely to influence the ways in which these groups will be able to complement these forms of illicit activities to sustain their provision of governance functions. What law enforcement measures and deterrence mechanisms need to be in place to avoid cyberspace from becoming a catalyst of conflict?

4. Further Emerging Questions

i. *Addressing the disconnect between security stakeholders.*

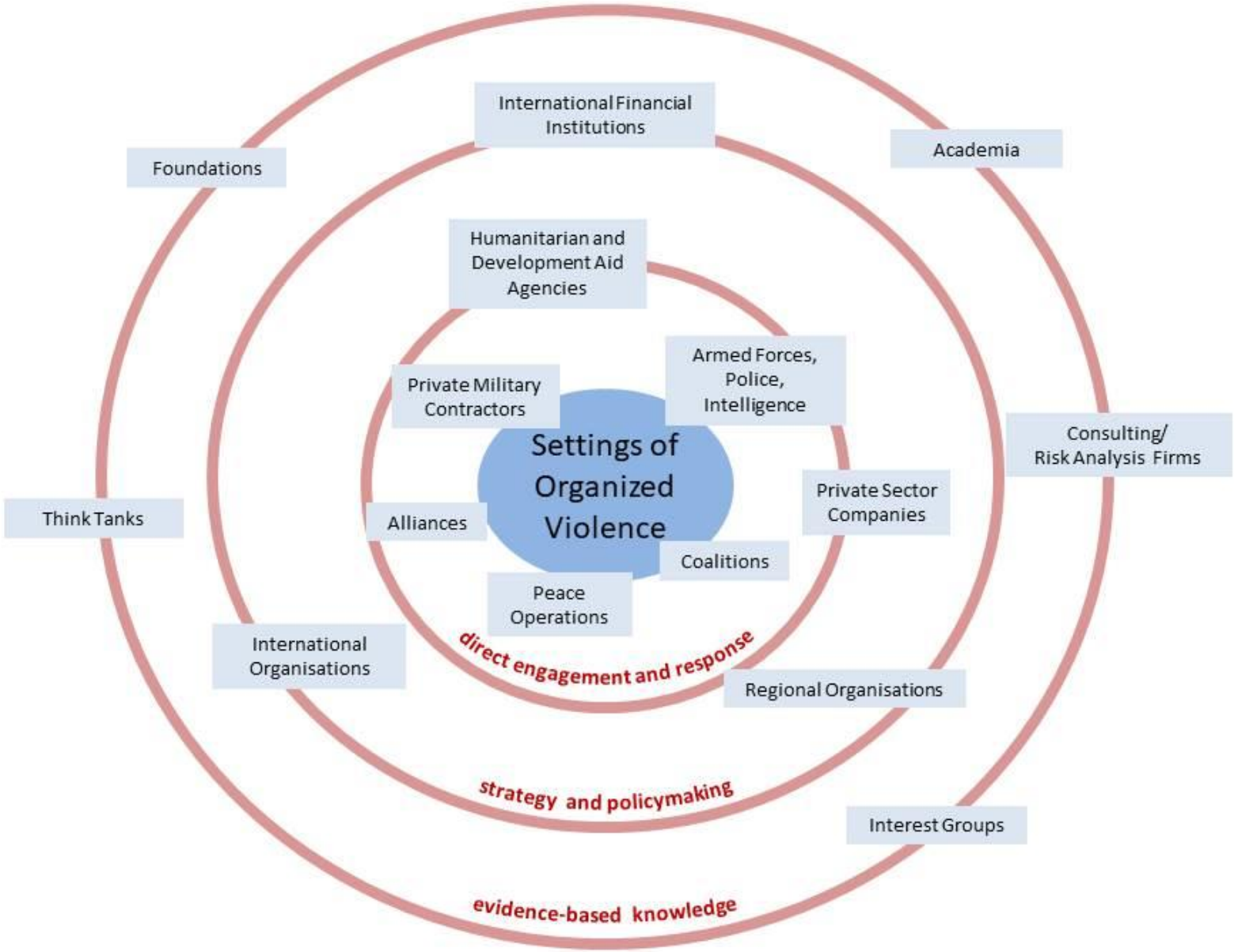
How can we foster interactions across all three levels of stakeholders?

ii. *Understanding perceptions.*

How can we move from an international security system that is largely framed around Western concepts of threats and responses to one that accounts for local perceptions (e.g. of governance provisions), promotes a global consensus, and thus tackles the current sense of exclusion and alienation of communities across the world?

iii. Encouraging prevention.

How can existing norms and largely static mechanisms be transformed from reactive approaches into proactive, flexible, networked measures that anticipate threats in order to prevent them?


International Financial Institutions
Academia
Foundations
Humanitarian and Development Aid Agencies
Armed Forces, Police, Intelligence
Private Military Contractors
Consulting/ Risk Analysis Firms
Settings of Organized Violence
Private Sector Companies
Think Tanks
Alliances
Coalitions
Peace Operations
direct engagement and response
International Organisations
Regional Organisations
strategy and policymaking
Interest Groups
evidence-based knowledge