The World Economic Forum Global Futures Council on The Future of International Security (2016-2018)

Contents

I. Parallel factors describing the context around the impact of the 4th Industrial Revolution

Global society and governance institutions are facing new challenges from an unfolding technological revolution that is fundamentally changing the way we live, work and interact with one another. The speed, scope and disruptive influence of this transformation is leaving slow-moving national governments scrambling to keep pace with the need to evolve and adapt institutions for the promotion of international security. The rising level of globalization in the last three decades has accelerated the impact of change, making it possible for billions of people to be connected by mobile devices with unprecedented processing power, storage capacity and access to knowledge. The capabilities that are emerging with related technologies of the Fourth Industrial Revolution (4IR), such as artificial intelligence, machine learning, robotics and biotechnology, have the potential to raise global income and improve the quality of life around the world. But they also can be used as tools to create great harm, allowing small countries and non-state actors to access the power to degrade global security and human well-being. Hacks to banking systems, medical establishments, electricity networks and national defense systems offer just one indication of the need for a new global architecture to address the dangers to come in the future of international security.

The World Economic Forum Council on the Future of international security will explore scenarios to reveal important and urgent areas for policy reform. Those scenarios will emphasize aspects of how the 4IR will transform international security. However, given the fact that International Security is subject to other trends developing in parallel with the impact of new technologies, the purpose of this paper is to identify some of those other main trends that are shaping the context in which the impact of the 4IR will occur.

Shifts in the balance of power

Having peaked in the late 20th century, the dominance of Western powers is gradually fading. Following the demise of the Soviet Union, the US led a unipolar international system for some time, but during Obama's presidency, China and Russia successfully challenged American geopolitical dominance in Europe, the Middle East and East Asia. Presidents Obama and Trump have each in different ways signaled that the United States will no longer sustain such a large share of the costs of leading the international order. At present, the United States is on course for a strategy that does not seek to bring about a global convergence on common principles, nor to bring peace to every corner of the world, or even to enforce common standards, but instead advances its own economic interests while managing conflicts with the two other major military powers (China and Russia).

Unprecedented levels of globalization in the last three decades were deeply favorable for the newly emerging (former Communist) economies and some developing countries. Formerly less-developed countries with the right mix of competitive factors have accumulated considerable wealth and secured an increasing share of the global consumer and investment markets. This rising economic power coupled with broadening interests have driven a shift of military power –

including power projection and access denial capacities - toward the non-western world, particularly in East Asia, but also in the Middle East and South Asia.

The current international order is structured around three assertive poles (the US, China and Russia), and the European Union (EU). As a community of 500 million relatively wealthy citizens, the EU is a considerable economic power, but struggles to emerge as a strategically autonomous actor on the geo-political stage mainly because it depends to such a large degree on the US for its defence. Although some EU members are exerting themselves to address this imbalance, the exit of the UK is a setback in this area, and leaves the EU even more exposed on the military front.

Russia`s economic standing is somewhere below that of other major powers, but its nuclear deterrent backs a military capability and doctrinal readiness to employ force, giving Moscow political and security options to shape outcomes in its neighborhood and areas of the Middle East. Russian leaders express exasperation with the US-led unipolar order, and have demonstrated its limits by asserting control in Russia`s neighbourhood, most recently in Georgia (2008) and Ukraine (2014).

China maintains claims in the region despite criticism that its approach disregards UNCLOS and its objection to freedom of navigation operations call into question its adherence to the international rules-based order. In comparison to Russia, China's economic stake in the global economic order make it in some ways a more cautious geopolitical player. President Xi`s defence of globalization at the last annual WEF meeting in January 2017 was qualified by his reference to *economic* globalization, the key elements of which are access to global markets, finance and technology. Such is the degree of economic interdependence, none of the parties objecting to the way China pursues it's maritime claims have raised the possibility of sanctions.

Meanwhile, through projects like its Belt and Road Initiative (BRI), and a steadily expanding area denial and power projection capabilities tipped with high-end military technologies, Beijing looks set to move into a position of regional dominance and global influence in areas of key strategic interest, such as the Indian Ocean, Persian Gulf, Africa and Latin America.

However, China's progress has triggered interest among neighbors Japan and India in developing more structured strategic cooperation, in both economic and military affairs. This initiative could become more significant if partners such as Australia, the USA or even Europeans were to take part. However, most of the countries concerned remain cautious not to allow such a hedging policy to inflame tensions with China. This is a reminder that an analysis of the global balance of power must also take into account second and third level actors. Africa, South Asia, Latin America are far more promising in projecting stability than at any time in the past. In Central and South America, a greater degree of integration is at work. A majority of Asian countries are mainly focused on an incremental process of improving their economic wellbeing.

Increased access to cyber technologies and weapons of mass destruction is leveling the playing field between greater and lesser world powers and threatening the balance of power system that has served as a deterrent to conflict in past decades.

For medium and small economies, it is essential to maintain stable relations with the United States and cultivate friendship with China. A large number of countries do not need Russia for

their economic survival or progress. However, Russia may serve as an alternative source of weapons procurement for some developing countries.

A final dimension of shifting power balances is demographic change. Countries like Japan are undergoing a dramatic population ageing and shrinkage of the working population. Some European countries and Russia are facing similar though less pronounced tendancies, which will impact their overall economic productivity as well as feed through into pressure to shift public spending towards social welfare. In contrast, areas of the Middle East and Africa have a youth boom, with attendant risks as well as benefits. The South Asian population continues to grow in both population and economic productivity. This too will affect long-term shifts in the international balance of power.

The features of this new geopolitical matrix where major powers are in a seesawing relationship are uncertainty, arms racing, saber-rattling, hedging and partnership-forming, and misinformation or other forms of psychological warfare. Although the US has overwhelming capacity for projection of military power compared to the other powers, its willingness to apply its strength is increasingly uncertain. The erosion of the global rules based order can be seen in the way that great power violations of the sovereignty of weaker states are increasingly likely to go unpunished.

No consensus on a legitimate world order

As the international distribution of power shifts, it exposes another dangerous trend: there is a lack of agreement on a legitimate world order.

In recent years some have portrayed Russia as pursuing a revisionist policy that puts Russian security above the sovereignty of its neighbors, and threatens peace in Europe. A contrasting narrative says it is the West, and particularly the United States, that has been reckless and self-seeking in its actions in Iraq, Libya and Syria. Western policy such as the expansion of NATO and support for colour revolutions are understood as moves to take advantage of Russia in a moment of weakness, and frustrate its rights as a major power. The invasion of Iraq is perhaps the clearest example used to discredit western claims to stand for a rules-based system.

The narrative of a ‘broken promise’ on NATO’s expansion sounds to some in Central Europe like a nostalgia for the days of Yalta and spheres of influence concept of world order. Similarly, China`s pursuit of territorial claims is viewed by some as betraying an approach to order that is unilateral and prone to disregard mechanisms of international law.

Just as Russia questions the justification for NATO, the US presence in the Western Pacific and its alliance system incorporating strong defence links with Japan, ROK, Taiwan, the Philippines, Australia and Thailand is viewed by some in China as an outdated relic of WWII, and the Cold War.

So as a model of world order we still have the UN Charter, but not the will to uphold it. We have contending structures of collective defence, whose legitimacy is called into question by their neighbours, who may go further to say such alliances run counter to international security. At the same time, alongside traditional alliances, we have new set of tools (cyber, digital media manipulation, transnational investment and regulatory regimes) with which to test the norm of non-interference in sovereign affairs. But at present, not one of the major powers nor any grouping of second or third tier powers are articulating a model of world order that satisfies their common interests to a level where it would command legitimacy.

Erosion of international norms

The breakdown of consensus on world order is being accompanied by erosion of support for the norms governing the use of force, protection of Human Rights, respect for International Humanitarian Law, and treatment of refugees.

Responsibility for this erosion is widely shared. Both Russia and China regularly stress their support for a rigorous interpretation of the UN charter on the use of force and the respect of the principle of national sovereignty, but China challenges the applicability of UNCLOS in the South China Sea and Russia uses hybrid warfare to circumvent limitations on the use of force. Meanwhile unilateral application of concepts like 'responsibility to protect' and the 'global war on terror' have been used to justify a loosening of the restrictions on the use of force by Western powers.

Added to this the legal framework that was agreed in 1945 has begun to diverge from the reality of modern conflict, which is characterized by the growing relevance of non-state actors, changes in the conventional battlefield, and the emergence of new battlefields (such as cyber). For instance, the humanitarian dimensions of the international security environment today are shaped by the protracted nature of armed conflicts, he prevalence of urban warfare, high levels of population displacement (that is being perceived in many countries through a security lens), increased humanitarian needs, connected populations using connectivity as an enabler to flee, etc. The use of asymmetric attacks to intelligence targets, political systems, intellectual property and financial networks has already negatively influenced the relationship among the great powers such as the United States, China and Russia.

The ICRC defines cyberwarfare as cyber operations against a computer or a computer network when used as means and method of warfare during an armed conflict. Where the belligerents recognize that IHL applies to cyber warfare, then the principles of distinction, proportionality and precautions do have the potential to protect critical civilian infrastructure in the cyber space, but there are a number of challenges, such as dual-use objects. The manner in which States will define the notion of attack will thus influence the level of protection that IHL grants to critical infrastructure. The ICRC holds the view that an operation designed to disable an object – for example a computer or a computer network – this operation is an attack for the rules on the conduct of hostilities, whether or not the object is disabled though kinetic or cyber means[1].

---

[1] The rules governing the conduct of hostilities provide special protection to some types of critical infrastructure, in particular medical facilities, objects indispensable to the survival of the population, like water networks, and objects containing dangerous forces, like nuclear power station. In the physical world, emblems and signs have been created to help belligerent identify objects benefiting from this special protection. Are there technical means to do the same in cyber space? Can it be done without increasing the vulnerability of these objects to attack by ill-minded people? The ICRC's IHL Challenges Report in 2015 highlighted "*This raises the question of the measures that States must take to protect the civilian population under their control from the danger of cyber operations, including in the case of a cyber operation against the State's essential infrastructure. Measures that could be considered include: segregating military from civilian cyber infrastructure and networks; segregating computer systems on which essential civilian infrastructure depends from the internet; backing up important civilian data; using antivirus measures; and making advance arrangements to ensure the timely repair of important computer systems against foreseeable kinds of cyber attacks.* ***Other avenues that could be explored – requiring international cooperation and, probably, innovative solutions to technical problems – would be to work on the identification in cyberspace of the cyber infrastructure and networks serving***

Mature globalization
A range of issues occurring at global scale are also responsible for shaping the trends of international security.

The effects of climate change on the drivers of conflict are more studied than agreed upon, but it seems clear from most models that continued or escalating climate change will cause large-scale and increasingly frequent disruptions in the basic life conditions of peoples all around the world. Effects on international security will in some cases be mediated by flood, crop failure, food insecurity, disease, etc. all of which are likely to trigger sudden massive movements of people. The current crisis of migration and refugee management is an early symptom of the difficulty most states and societies have in adapting to these unplanned aspects of a borderless world.

The global nature of public debt markets, investment and trade regimes mean that 'domestic' growth and jobs are increasingly dependent on policy choices in other countries. There is a backlash emerging whereby investment flows formerly seen as the lifeblood of economic globalization that would 'raise all boats' is increasingly criticized as a form of 'interference' in sovereign affairs, against which governments should be protecting the jobs and wellbeing of their citizens.

Automation is increasingly transforming the labour markets, in ways that are still heavily debated. Many fear the impact of technology will be to eliminate jobs and intensify the politicization of economic competition, e.g. through protectionist policies as social protection. The decoupling between wealth and labour is accelerating. Income inequalities continue to increase; there is also growing awareness amongst the "have nots" of the wealth of the "haves";

Reconfiguration of domestic politics and the crisis of the state
Karl Marx wrote in the Communist Manifesto: "the working men have no country", but today it is the opposite: the workers, unless they choose the desperate path of migration, are stuck in their country, and the globalists are the members of the wealthy elite, who can find jobs anywhere. This has implications for the **social compact** that emerged in the twentieth century, when the upper classes had to accept income redistribution through very progressive tax systems. Today internal **inequality** is on the rise in western countries, but also in China or Russia, where it reaches extreme levels.

We have seen an increasing role of the masses not only in the internal policy, but also in foreign affairs. There are a lot of reasons: migration, the disintegration of traditional societies, new technologies, especially in the telecommunication sphere. The economic outcomes of globalization in the post-Cold War era yielded adverse economic and political implications in Western Europe and the United States. As a result, the traditional political elites are losing their influence almost everywhere. Political leaders and the institutions of government have decreasing ability to effect change. The former **parties** and **ideological structures** are

---

***specially protected objects like hospitals**, or to draw inspiration from the protection attached to demilitarized or protected zones and to assess whether such an approach could usefully be transposed into the cyber realm."*

becoming meaningless. In their place comes either anti-elite populist movements, or new elite associations.

PR-savvy politicians who project an image of strength and who can provide reassurances to people through soundbites and simple messages are in the ascendant. The reinvigoration of right leaning parties in the Western world with their protectionist and nationalist policies is an indication of the imbalances that the process of globalization created. Either may be founded as the response to the indiscriminate fears of the masses. As a result we can see a potentially very speedy process of the fragmentation of the societies. It is a serious challenge for international security.[2]

Empowerment of the individual

States may be facing a long-term threat, but the more immediate consequence of globalization and the internet revolution has been an extraordinary empowerment of the individual, which has made the last three decades among the best in the history of humanity, lifting hundreds of millions out of poverty. The geopolitical consequences of what one could call a "disintermediation" of human destiny are hard to ascertain. Mediating institutions such as states, are, like major financial institutions, a potential risk factor as they concentrate power ("too big to fail") as well as a risk management tool, acting as buffers, and pooling risks. A world of increasingly empowered individuals is potentially more dynamic and more fluid, but also more unpredictable. It needs structures to mediate, organize and standardize their interactions, but lacks the socio-political foundations on which to build them. And international institutions face a crisis if the states that are their building blocks are themselves in crisis.

It is in this context that citizens are experiencing a new insecurity that the pact between government and the governed is breaking down in many places in the world. As technology has eliminated jobs, the increasingly shaky global economic system has yielded adverse economic and political implications in many regions of the world. The rise of a zero sum geo-economic narrative is reinvigorating nationalist movements with their protectionist and socially exclusionary policies.

The empowerment of the individual signals the **demise of ideologies** that emphasized the collective dimension of human destiny, and opens a vacuum: the pursuit of money and the triumph of individual agency are at once powerful drivers of economic growth and dangerous solvents of the social fabric.

In a world largely defined by material success, there is a **thirst for values**, especially when material success is a remote prospect. Meanwhile, the internet revolution redefines social dynamics, allowing for new **non-territorial solidarities** of trans-national communities (for instance, importance of internet in recruitment of jihadists). That vacuum is being filled by a revival of **nationalism**, religious fanaticism, or both, depending on the countries. Identity is increasingly multi-layered, globalised, and shaped by social media; this is celebrated by some and vilified by others. Echo chambers are becoming the main opinion formers: social media are becoming the dominant source of news/information. It also facilitates the fragmentation of society into closed, self-referential groups, hence the increased polarization of politics in western societies.

---

[2] The last report of the Valdai International Discussion Club called "**The Global revolt** …"

People are increasingly “hooked” on virtual reality, and other ICT; this is having as yet poorly understood impacts on cognitive and behavioral skills, and is changing how people interact with one another;

Non-state actors and a more ‘bottom-up’ world

These various trends combine to challenge a traditional top-down understanding of the geopolitical situation. States, including the major powers, are not independent self-contained actors on an international chessboard. They are being pulled apart by subnational as well as transnational forces, and conflict dynamics are profoundly transformed in several ways: 1/ Conflicts are increasingly difficult to isolate from a broader context, which makes their resolution more difficult: they often have a local, regional, global and transnational dimension. Addressing all those dimensions at once is almost impossible. 2/ while external actors are often involved, few wars are pure proxy wars. All actors have some autonomy, which increases the risk of uncontrolled escalation, as global or regional actors do not have full control over local actors, but are sufficiently connected to be drawn into wars that are not their owns. 3/ International politics are driven by domestic dynamics that stand in the way of conflict resolution (best example is sixteen years of flawed counter-terrorism strategies) 4/Goals of conflict actors are increasingly difficult to accommodate in a political settlement, either because they are irreconcilable (I.e. transnational terrorist organizations), or because conflict actors have no interest in the resolution of the conflict (criminal actors).

Approaches to internatinal security need to pay more attention to nongovernment international actors such as transnational business corporations, humanitarian organizations, international professional communities etc. The new information-communication environment gives the great opportunities for such kind actors to obtain a new role in the modern world.

Growth of criminal networks

The crisis of politics and the accompanying weakening of the state blur the line that should separate crime and politics. In an increasing number of situations, criminal agendas and political agendas are intertwined, as criminal actors thrive on low-intensity conflict that erodes the capacity of state institutions to enforce laws. Criminal actors often have more resources than weak states starved for funds, and they can take over state institutions, further delegitimizing them.

Terrorism a symptom of structural weaknesses, rather than a strategic threat in itself

For a while Al Qaeda was seen by many as the strategic threat to be defeated. The Islamic State is now seen as the enemy number one, although Al Qaeda is alive and well in several countries. It is likely that ISIS will eventually be defeated, but some other organization will then emerge. In Muslim countries, Islamic terrorism needs the chaos of war – that destroys state structures - to prosper. In western countries, its impact is significant only because of the fragility of western societies in which the politics of fear magnify an otherwise very limited physical impact. Focusing on terrorism – which is a tactic – as a strategic threat, is a self-fulfilling policy that makes it more attractive to individuals who then become part of a global narrative that transcends their personal circumstances and gives a broader meaning to their actions.

Extreme (predominantly Islamist, but not only) terrorist organisations are using unprecedented violence as a means of attracting global followership and funding. Terrorists/criminals/rogue states have access to unprecedented means of mass destruction (bioweapons, cyber weapons, etc)

Coping mechanisms

The main characteristic of this world is that while the multiplication of grand conferences (G2, G7, G20,…) maintains the appearance of a top-down controlled world, there is actually very little control over unfolding events. It is not a G-0 world, but rather a multi-layered world with a multiplicity of influencers, in which traditional structures (states, international institutions) compete with new actors, with positive as well as negative agendas (individuals, corporations, NGOs, criminal networks, terrorist organizations).

How that competition will be settled and which institutions will then emerge is unknown. At the time of the Renaissance, it took a century of wars in Europe for the nation-state to emerge. In an age of nuclear weapons, it is of critical importance that the emergence of a new order does not happen through wars, as it is presently happening in the Middle East. The most important priority should therefore be to maintain a body of international law that helps regulate the use of force and contain the spread of war, while new structures gradually emerge.

The Persian Gulf region has experienced three wars in the last four decades yet the UAE, Qatar and to some degree Saudi Arabia have demonstrated remarkable levels of economic growth and prosperity. Geopolitical tensions if managed well may not interfere with economic development if all parties correlate their perceptions and estimations. The underlying logic for this conclusion may be that a global self-regulated political and geopolitical order may not be on the horizon. In a geopolitical environment characterized by **short-term to medium-term calculations, constant oscillations and maneuvering playbooks, it** may be rather misleading to anticipate the return of a single international security system.

Instead regionalism and processes of regionalization may be more appropriate to fit the realities of geopolitical competition. Compared to 1945 and 1990 global contexts, the US or any other would-be global hegemon may expect to encounter resistance to the global security and geopolitical norms it wishes to institutionalize.

II. Challenges for Responses across the World's Changing Security Landscape

Discussion paper prepared for the WEF's Global Future Council on International Security
Dr Annette Idler, University of Oxford, November 2017

This paper discusses the actors, mechanisms, and norms which compose the current international security architecture to enhance understanding on how threats to the global public good 'international security' are being prevented, anticipated, and responded to. It identifies challenges in the current system with a view to developing a strategy to transform the current system into a more efficient and reliable one that is 'fit-for-purpose' to address the security challenges of the 21st century.

1. Stakeholders in International Security

The paper is based on the WEF's Global Future Council definition of 'international security' as the system of policies, norms and multi-stakeholder collaborations that minimise the likelihood and consequences of organised violence [original wording: conflict] between states and/or non-state actors. To operationalise the definition, below is a list of main actors directly or indirectly participating in organised violence to illustrate the variety of potential stakeholders (rather than being exhaustive).

State Actors	**Non-state Actors**
- Governments (including armed forces, police, intelligence) - International Organisations (e.g. UN Peacekeeping Missions) - Regional Organisations (e.g. African Union, European Union) - Alliances (long-term) (e.g. NATO) - Coalitions (temporary) (e.g. Global Coalition against Daesh) - …	- Insurgent groups - Separatists - Terrorist organisations - Paramilitaries - Organised criminals ▪ hacking groups ▪ gangs ▪ pirates ▪ mercenaries ▪ drug cartels - Foreign fighters - ….

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 organised violence;
ii. actors involved in the policymaking process and strategic planning;

iii. actors developing the evidence base and wider knowledge on settings of organised violence that other stakeholder groups draw on.

The graph in the annex visualises these three stakeholder groups as inner, intermediate, and outer rings to threats to international security. The distinction between those fuelling/participating in conflict and those responding to, or aiming to mitigate it is often 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. This divergence of perceptions is currently hardly accounted for in discussions on reforming or transforming the international security architecture.

2. Norms and Mechanisms as Responses

The norms and mechanisms developed to maintain the common public good of international security are mostly being developed at the second level. The principal mechanisms are:

- 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 targets, such as Sustainable Development Goal 16, norms and approaches, such as Responsibility to Protect and the upholding of Human Security; and further responsive mechanisms such as sanctions.

These norms and mechanisms have evolved in parallel with the 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 wide array of issues addressed through them, ranging from deterrence of state attacks, and the protection of civilians in armed conflict, to mechanisms to avoid that weapons of mass destruction fall into the hands of terrorists.

While the norms and response mechanisms account for the existence of the increasing diversity in actors relevant to the international security system, they manifest shortcomings in anticipating and tackling the modus operandi of the state and non-state actors who engage in organised violence. Based on traditional conflict measures such as the number of battle deaths, most assume a state-centric approach in assessing threats to security and determining thresholds for when, where, and how to respond. As a result, security policies continue to adopt reactive approaches rather than to anticipate future changes in conflict; this concerns the international, regional, and national level. For instance, in Haiti, UN Peacekeeping operations had a civil war approach even though the dynamics were intertwined with criminal violence. In Afghanistan and Iraq, the international intervention followed a counterinsurgency paradigm, neglecting hybrid methods in war. In Ukraine, governments underestimated the manipulation through social media with which governments influenced local communities. In Colombia, the post-conflict strategy prioritises the demobilised rebels, even though multiple violent non-state groups continue to shape the security landscape. Rather than the absence of norms and mechanisms, it is their erosion in the face of the current security threats, which requires rethinking.

3. Five Challenges to the International Security Architecture

Against the backdrop of the existing actors, norms, and mechanisms that make up the international security system, this section gives an overview of key challenges that changes in the principal security actors pose to our response mechanisms. These are driven by a variety of wider trends including those linked to geopolitical shifts, demographic pressures, an increasing disconnect between power centres and communities at the margins, as well as emerging technologies. Geopolitical shifts give rise to questions such as whether the UN Security Council's current form is obsolete, and demographic pressures point to issues such as 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 focus here is on the last two trends. The challenges concern each of five dimensions of change in conflict: actors, impact, environments, methods, and resources.

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 together. By way of example, in the eastern parts of the Democratic Republic of Congo there are more than seventy different groups, in Libya, there are hundreds, and, according to the Carter Center, in Syria around seven thousand groups claim their presence. The proliferation of violent non-state groups poses challenges for our responses. What kind of groups should international organisations engage with, and if so, how? The International Committee of the Red Cross and the United Nations are only starting to develop thinking on groups such as gangs, militias and other non-state actors. 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 be seen as a relevant stakeholder on the security map. What does this proliferation mean for norms related to the recognition of groups?

ii. What (Impact): Violence versus Illicit Governance

International attention on conflict actors such as Daesh focuses on their violent behaviour, neglecting the ability of such groups to exercise authority and to assume governance functions including the provision of basic services and of competitive illicit economic alternatives. A large variety of armed actors is involved in such control over civilians: religiously motivated groups such as Al Qaeda in Iraq and Taliban in Afghanistan; ethnically motivated groups such as LRA in the Congo; 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, are nothing new. State-like forms of governance where groups tax populations, issue ID cards or set up check points on roads exist across the globe. Yet the modus operandi of such groups has been changing, and is likely to change further in the future, with a significant impact on state-society relations. In a time when central power holders are in crisis, such groups are perceived to be "legitimate authorities", eroding states from within and fragmenting governance across territories. How can outside interventions account for such perceptions where communities are alienated from states to avoid an expansion of safe havens and illicit economies? How can we move from a mainly military-centred approach to inclusive security policies?

iii. Where (Environments): Transnationality and Cyberspace

Conflict actors operate increasingly transnationally, posing challenges to peace and security on three levels. Locally, by jeopardising the physical security of local communities; regionally, by producing "problems without passports" such as refugee flows and threats linked to transnational organised crime; and globally, by using ungoverned spaces as safe havens for terrorism. By doing so, they challenge the entire state system rather than single governments. As means of virtual communication become more easily accessible, the transnational modus operandi of non-state armed groups is also likely to increase. The cyberspace itself has become another conflict theatre that conflict actors 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 the cyberspace as a non-physical space that is least integrated into our responses?

iv. How (Methods): Interconnectedness and Information Technologies

Changes in the modus operandi of conflict actors (both non-state actors, and state actors drawing on proxies, or cooperating with non-state actors) concern two major areas: first, the increasing interconnectedness; second, the access to emerging technologies. Conflict actors operate in an increasingly interconnected manner, yet the norms and mechanisms that the international security has established 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 actors involved in them 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 conflict actors operating in quickly shifting alliances and resilient, networked structures?

Access to emerging technologies not only facilitates networked structures, but also consolidating support globally. The increasingly easy access to technology has led to an unprecedented acceleration of the spread of information across the world. Conflict actors 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 want to communicate to their supporters or opponents. As information becomes increasingly accessible, marginalized communities are also increasingly 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 can lead to more violent conflict, or they can be channeled by non-state armed groups into 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 the cyber space. Non-state armed 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 to the 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 more 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 the cyber space from becoming a catalyst of conflict?

4. Further Emerging Questions

i. *Addressing the disconnect between security stakeholders.*

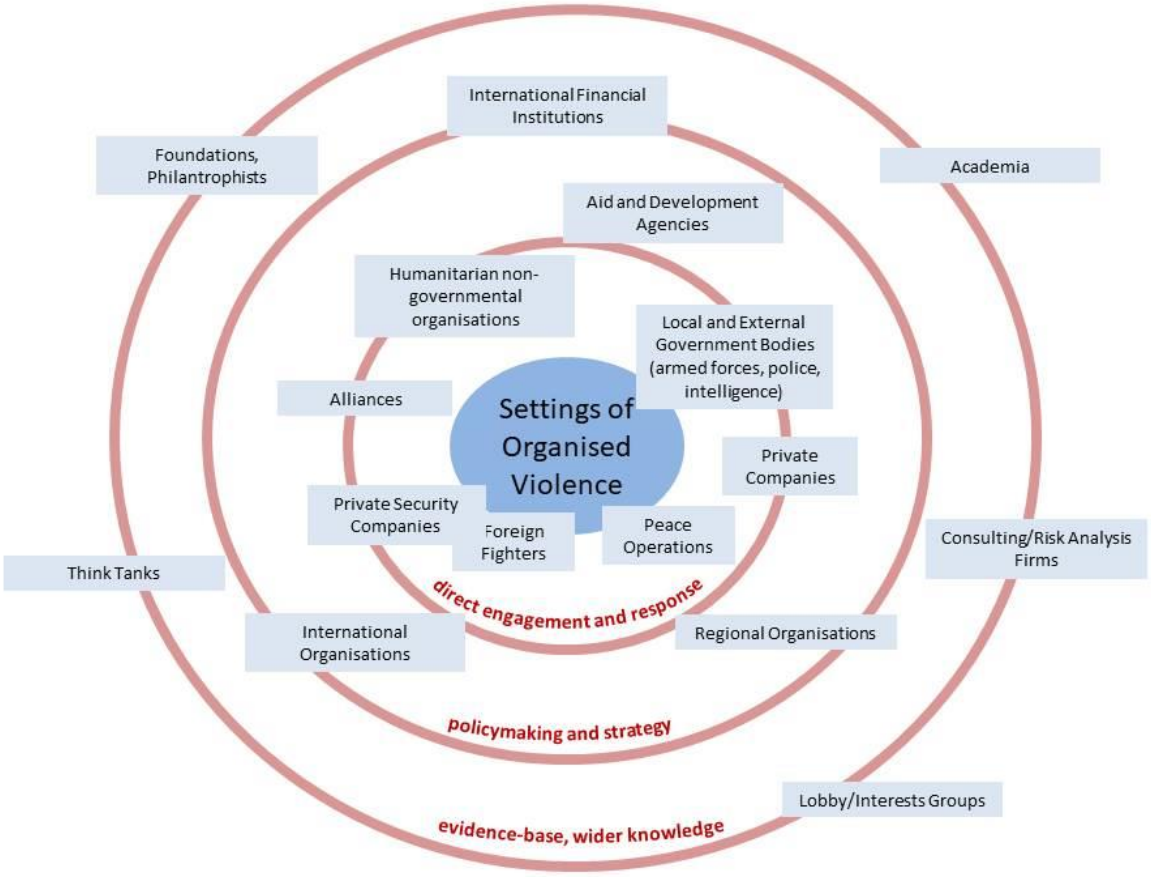
How can we foster interactions across all three levels of stakeholders?

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?

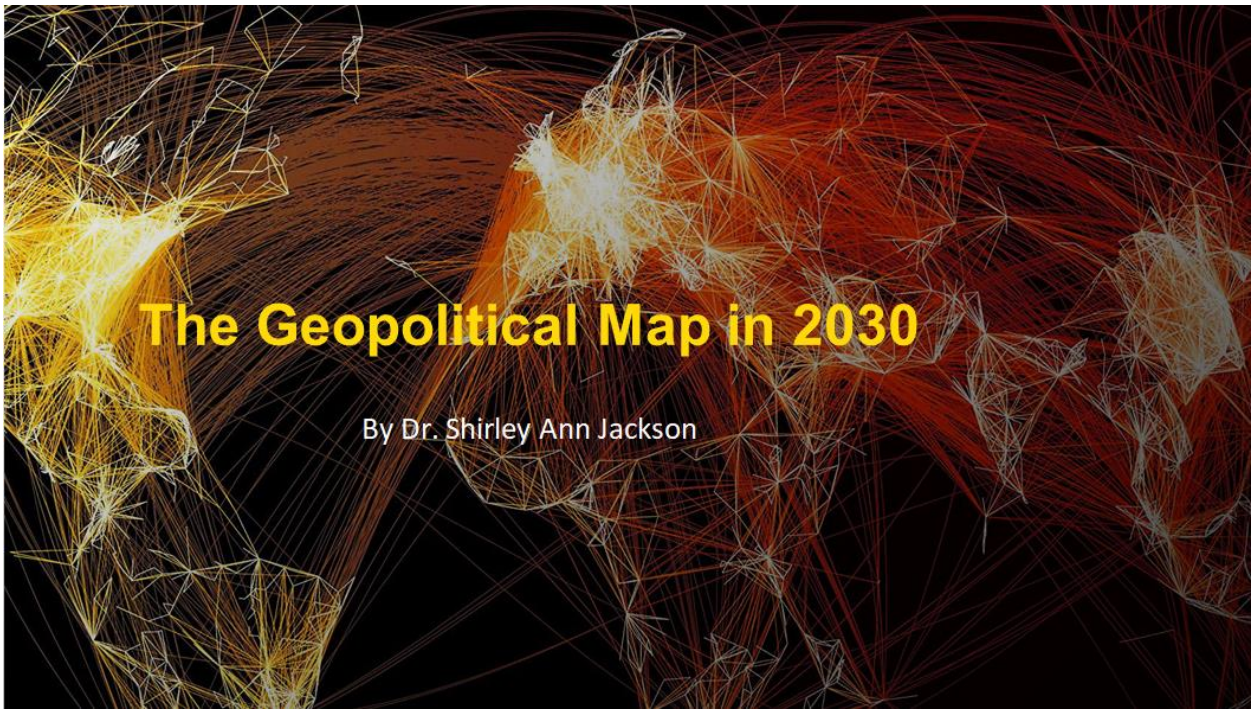
iii. Encouraging prevention.

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


International Financial Institutions
Foundations, Philantrophists
Academia
Aid and Development Agencies
Humanitarian non-governmental organisations
Local and External Government Bodies (armed forces, police, intelligence)
Alliances
Settings of Organised Violence
Private Companies
Private Security Companies
Foreign Fighters
Peace Operations
Consulting/Risk Analysis Firms
Think Tanks
direct engagement and response
International Organisations
Regional Organisations
policymaking and strategy
Lobby/Interests Groups
evidence-base, wider knowledge

III. The Geopolitical Map in 2030

Introduction
Now, we will look a dozen years into the future—when changes in the energy landscape; climate change; diverging demographics between the developed and the developing world**;** and powerful new technologies will create intersecting vulnerabilities—and opportunities—with potentially cascading consequences. These vulnerabilities and opportunities may well transcend geography, and alter old alliances and trading routes.



- The era following the Cold War in which the United States led the international order is coming to a close.

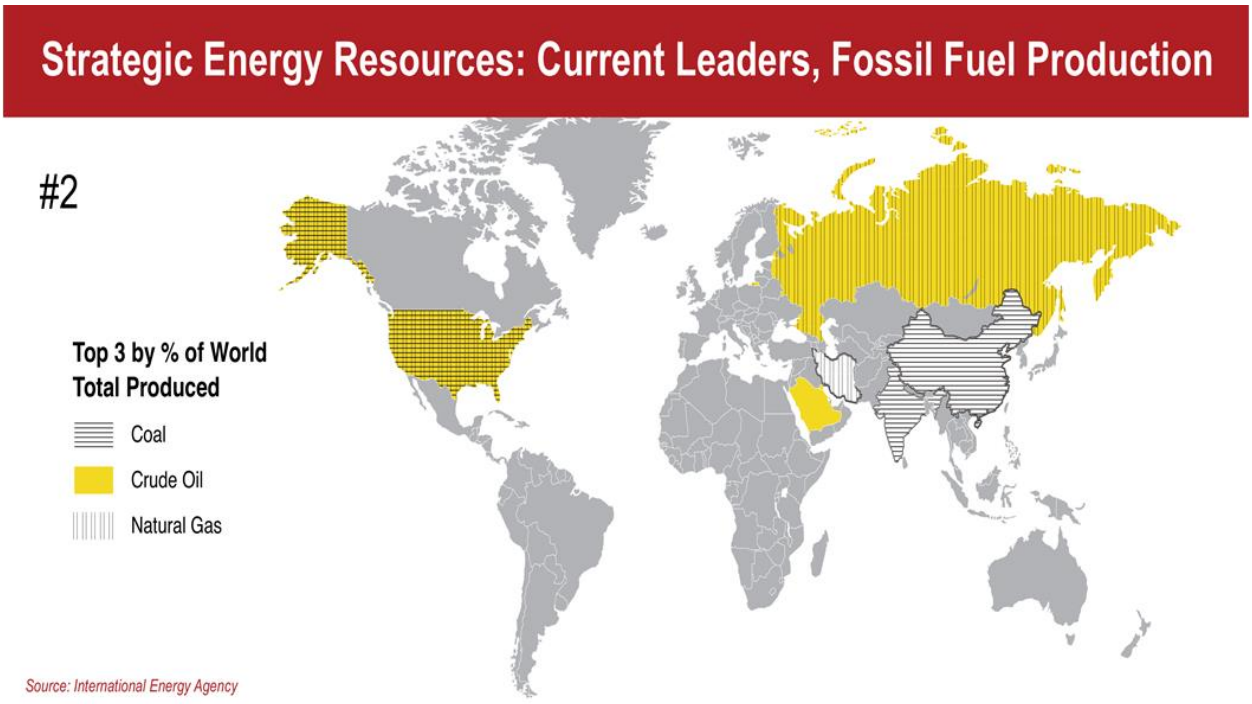
- Russia and China are exerting regional power—and by 2030, there will be a new degree of economic power in emerging economies, including Nigeria, Iran, Brazil, Indonesia, Mexico, and Turkey. And the speed at which they are emerging is unprecedented. Globally, over 2 billion more people will enter the middle class by 2030.

- However, it is not merely GDP that determines geopolitical power. Also key are access to, and control of, key strategic resources—especially energy-related resources; human capital; and connectivity in terms of technology and trade.

- So let us consider the ways that the forces unleashed by the Fourth Industrial Revolution will rewrite the geopolitical maps by 2030.

Major economic powers in 2030

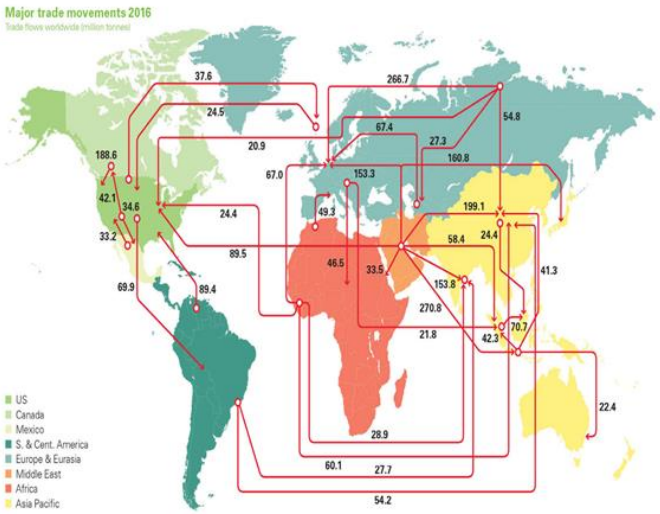
Strategic Energy Resources



- There is no development without energy, which today remains very linked to fossil fuels, and countries derive power from that.

Oil Supply Movements Across Geographies

#3



Source: BP Statistical Review of World Energy June 2017

- Oil and natural gas also create complex trading relationships, both within and in defiance of regional boundaries. Russia is rich in natural gas and oil, and has used those riches to geopolitical advantage, e.g. in the Ukraine and the EU.

- But we are moving to a low-carbon world, which is driven by climate change; steep cost reductions in, and access to, renewable energy; as well as by purely geopolitical concerns—such as a desire to loosen any one country's grip on another. As Russia becomes more aggressive towards the West, (including allegedly interfering in democratic elections in the U.S. and Europe), other sources of energy offer Europe the prospect of cutting its imports of gas and oil from Russia
- Around the world, more energy will be produced locally—including off-grid renewable energy that will bring power to those who do not yet have access to electricity.

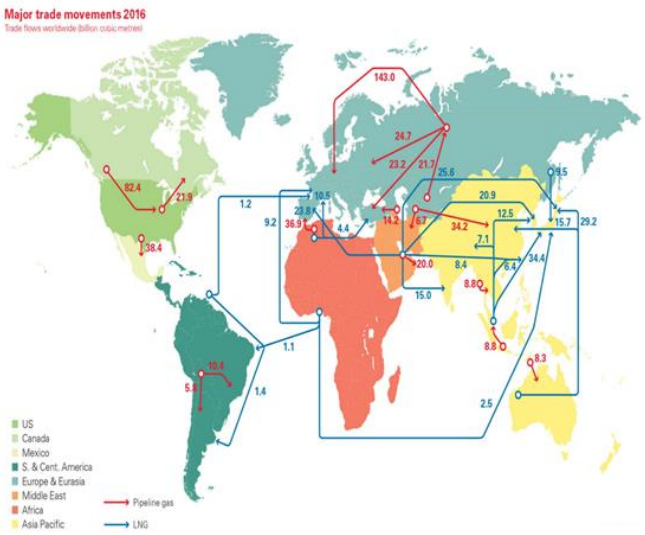
- Let us look more closely at China. The International Energy Agency expects global renewable energy capacity to expand by 43% between 2017 and 2022, driven by upward revisions of solar capacity in China and India. China alone will be responsible for 40% of global renewable capacity growth.

- China's Thirteenth Five-Year Plan, ratified by the National People's Congress in 2016, positions the nation for even greater power in a low-carbon world. Its key themes include…

- a focus on innovation to steer growth,
- ensuring that this growth is green and sustainable,
- regional coordination and inclusion of all Chinese in growth,
- and openness to trade—represented by its One Belt, One Road plan—to help create the infrastructure for an overland trade route to Europe through Iran, already a key trading partner for oil, and a maritime Silk Road. The program encompasses 65 countries representing 40% of global GDP. This represents a continuation of China's longstanding policy of trading or developing infrastructure for access to key markets and resources.
- In a low-carbon world, the most critical strategic resources will be different. This will be a materials-based revolution, with new struggles for access and control of non-fuel mineral resources.

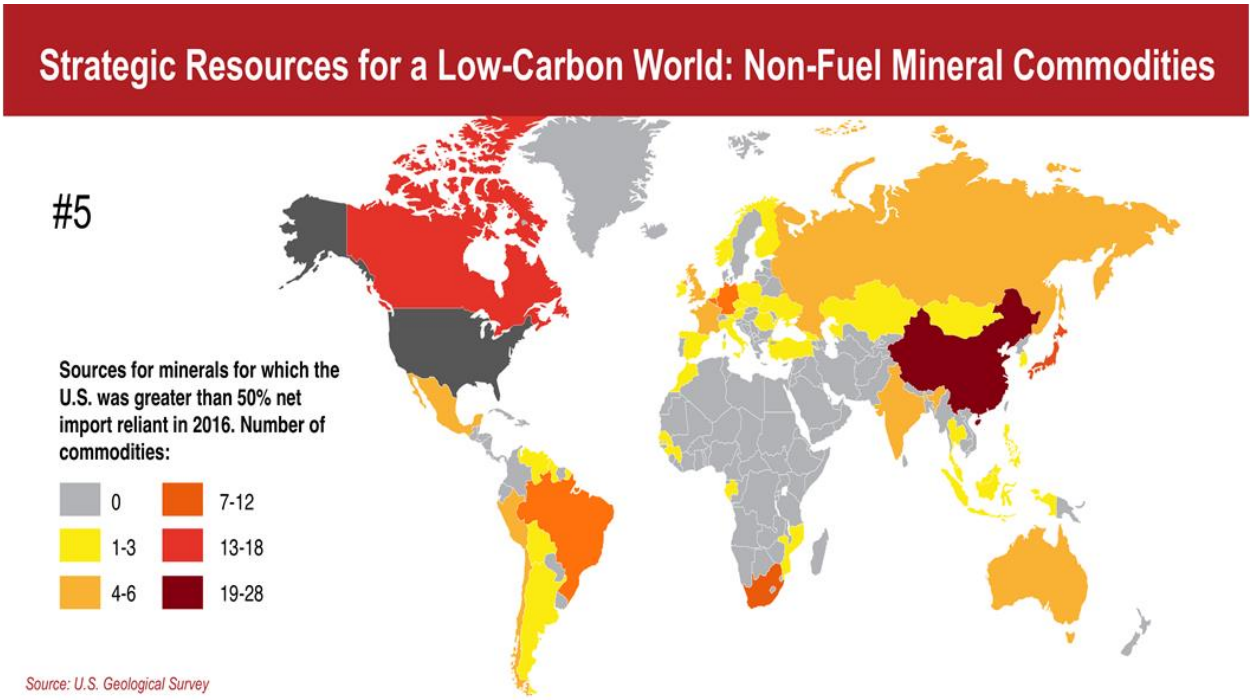
Natural Gas Supply Movements Across Geographies

#4



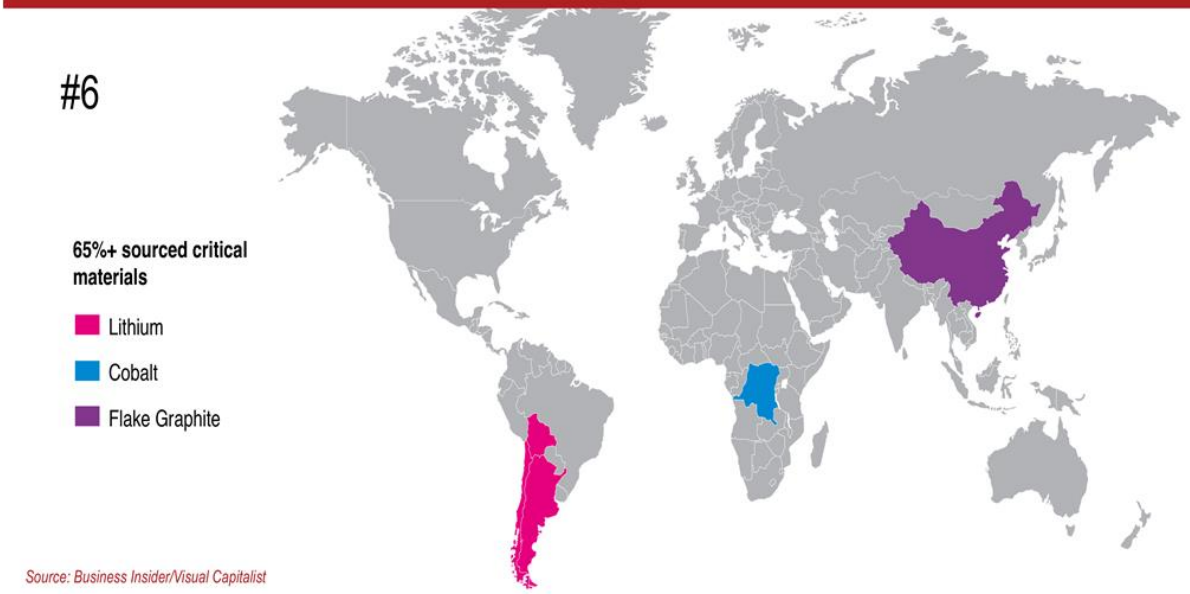
Source: BP Statistical Review of World Energy June 2017

Non-fuel Mineral Resources



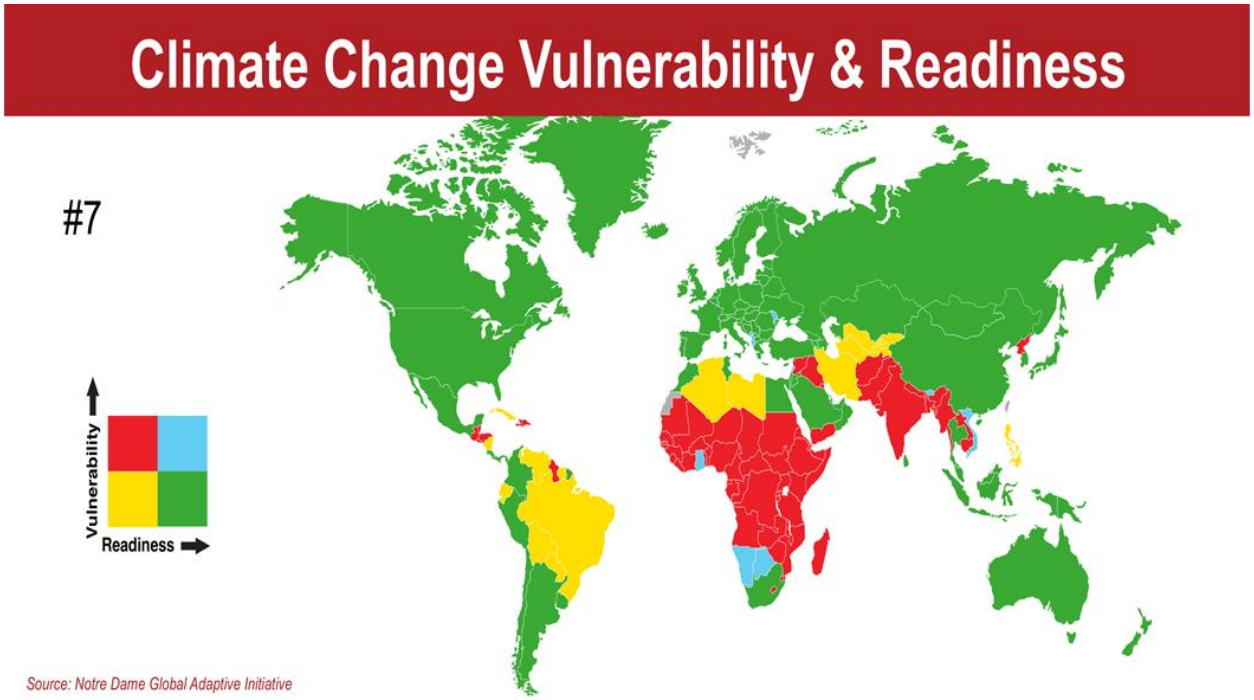
- For example, this U.S. Geological Survey map suggests the degree to which the United States is dependent on China for mineral commodities that are essential in technology, security, and energy.

Strategic Resources: Lithium-Ion Batteries



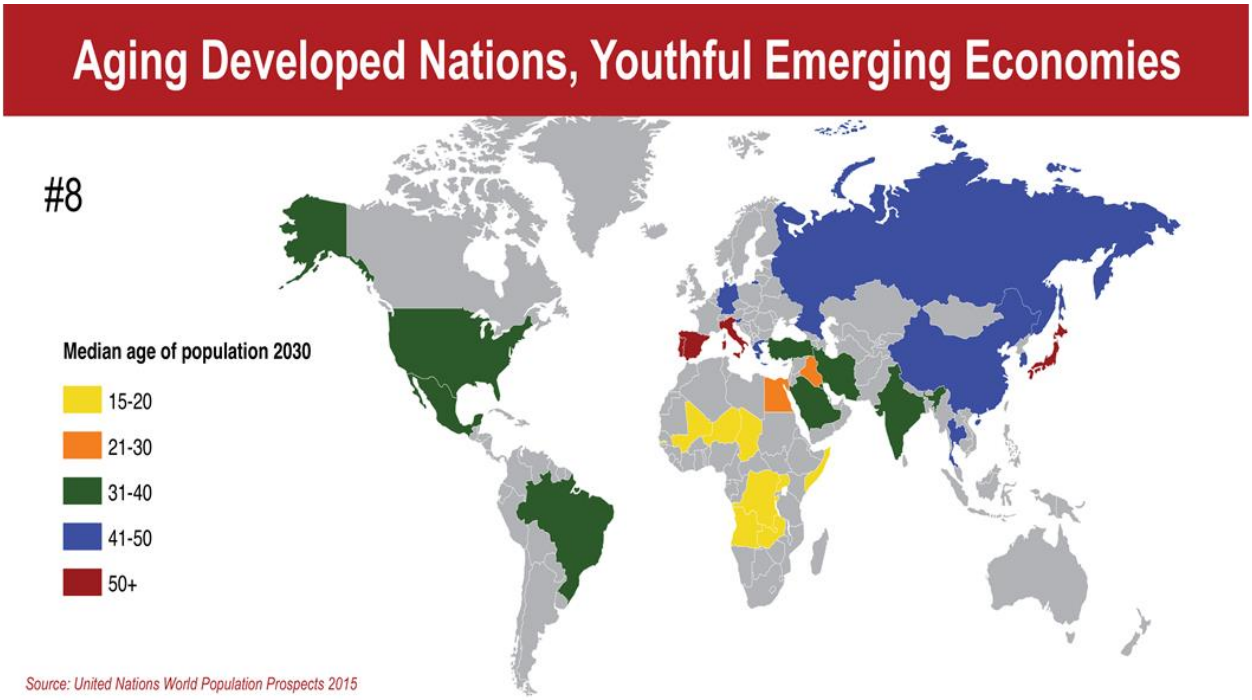
- As the transportation sector moves towards electrification, critical resources include key materials for lithium ion-batteries currently produced in a very few nations: 75% of lithium is mined in Chile, Argentina, and Bolivia; 65% of cobalt is mined in the conflict-ridden Democratic Republic of the Congo; and 65% of flake graphite is mined in China. There are potentially catastrophic price shocks and security risks if the supply chains for these materials are disrupted, absent diversification or the development of substitute materials.

Climate Change vulnerability and readiness

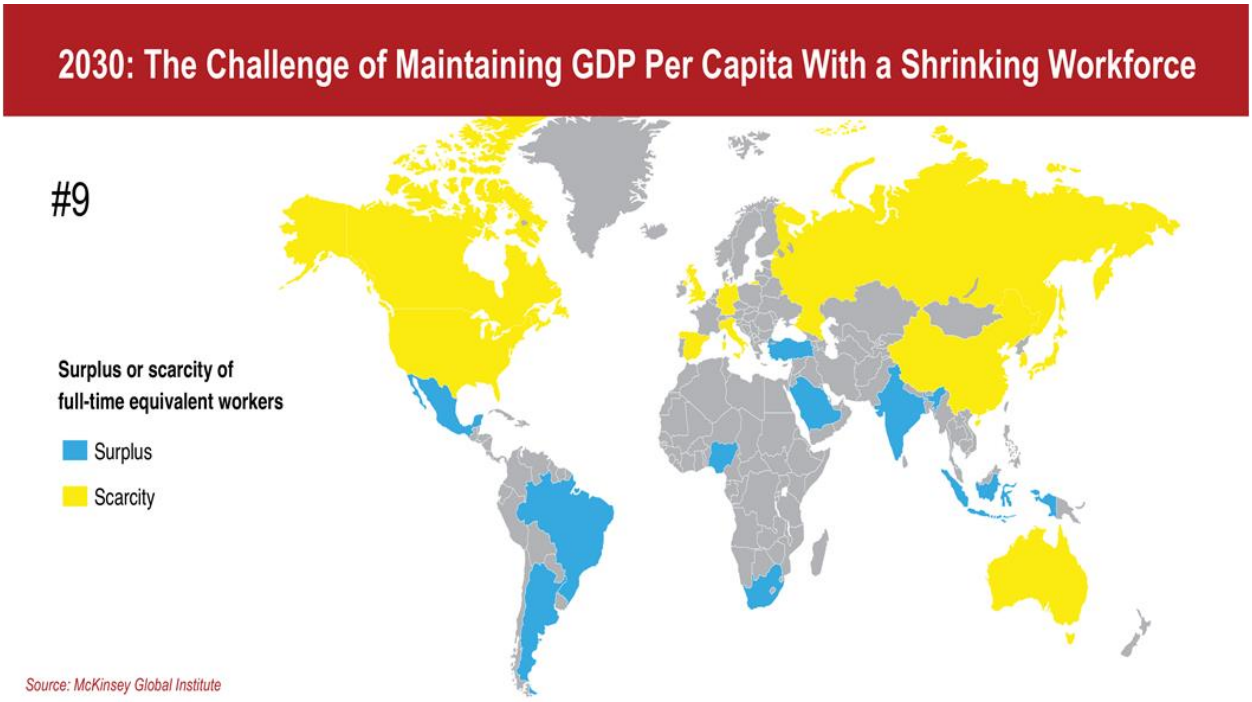


- Climate change will bring on its own security risks.
- While the risks to Africa include threats to rain-fed agriculture due to drought, both India and China have low-elevation coastal cities vulnerable to sea-level rises and storm surges—cities such as Guangzhou and Shenzhen, and Mumbai and Kolkata.
- The potential for intersecting vulnerabilities with cascading consequences is high. Is climate change going to drive migrations beyond recent refugee crises? Encourage the spread of infectious diseases? Increase dissatisfaction with the performance of governments in vulnerable regions such as South Asia, and encourage instability? Disrupt global supply chains? Alter access to key resources?
- For example, shrinking ice cover in the Arctic Circle is opening new resources and trade routes to exploitation—including an estimated 30% of undiscovered conventional natural gas reserves and 13% of undiscovered conventional oil reserves. Control of these resources and routes is likely to be a source of geopolitical tensions between the U.S., Russia, and other nations.

Human Resources



- Another key component of geopolitical power is human resources. The world population will grow from 7.6 billion today to 8.5 billion by 2030. India soon will overtake China as the most populous country. By 2050, Nigeria will overtake the United States to become the third most populous nation on Earth.



- The world is diverging demographically, with the developed world aging and the developing world experiencing a youth boom. In 2030, the divides are extreme—with much of Africa having a median population age under 20, while countries in Europe, China, Russia, and Japan have median ages more than twice that.

- For the developed world, a scarcity of full-time workers will make it challenging to maintain GDP growth.

- Productivity growth, possibly brought on by advances in artificial intelligence and robotics, may be key here. At the same time, automation and AI may exacerbate the decoupling of economic growth from employment, increasing the share of GDP that goes to capital rather than labor, thereby increasing inequality within societies.

- India, Pakistan, Egypt, Nigeria, and Kenya all will have growing working age populations between 15 and 64. This could be a great economic benefit. But do they have the opportunities, education, and infrastructure to take advantage of it? A challenge to rising living standards: Working age populations will grow the most in South Asian and African countries where average education levels are among the lowest.

- India will have 10 million new working age residents per year in the coming decades—but needs to improve its energy, manufacturing, and transportation infrastructure to accommodate this growth. The contrast between India's thriving technology sector and its less spectacular manufacturing sector suggests the gap

between the excellent elite education it offers in its universities—and poor overall basic education. It also suggests a broader entrepreneurship and productivity gap in the industrial sector, once one moves beyond IT and pharmaceuticals.

- Both India and China will have another challenge to social stability, as cultural preferences for boys have skewed sex ratios in their favor.

- Recent history suggests that states with youthful populations—and insufficient opportunities—are the most prone to intra-state political violence. In the Middle East, large youth populations, and the failure of governments in Egypt, Syria, Libya, Yemen, and Iraq to provide sufficient opportunities, have encouraged instability.

- The migrations provoked by such instability—in combination with the sense that globalization has not benefitted the middle classes in the developing world—are a source of geopolitical tensions, and are responsible for a new nationalism in the U.S. and the E.U.

- Yet migrations can offer a long-term benefit to nations with aging and shrinking populations. Because of immigration, the United States is not projected to grow as old as nations such as Russia, Italy, Germany, Spain, and Japan: The United Nations predicts a median age of 40 in 2030. But will current policy changes alter that trajectory? Net migration is projected to account for 82 percent of population growth in high-income countries by 2050.

- And developed nations with aging populations may find that their people do not have the skills required to create and to use the technologies of the future.

Technology and Innovation

- Can technology enable intergenerational linkages in ways that create greater productivity and innovation, and thereby confer economic strength by virtue of building economies that simultaneously take advantage of the forward-thinking and risk-taking of the young, and the wisdom and experience of older populations? This will require a new kind of intergenerational contract that has yet to evolve. :

- One challenge is clear; Technology is making governing more difficult. Technological diffusion—and communications connectivity—can lead to social control slipping away from the primacy of the state, in several directions at once.

- It allows transnational alliances such as alliances of multi-national corporations, non-governmental organizations (NGOs), or other multi-lateral organizations, at one end of the spectrum—or transnational terrorist or criminal groups at the other end. It allows, as well, internal groups, including cities and states, to challenge central governments and to create instability without large militaries, economies, or populations. The increasing expectations of a rising global middle class may fuel

dissatisfaction with the prevailing leadership—and provoke instability—and mass displacements of people.

- Of course, this shift is not merely due to connectivity—but also to the fact that many technologies of the Fourth Industrial Revolution can be easily weaponized by non-state actors. ISIS used commercial drones to carry bombs in Mosul; grenade launchers can be manufactured using 3-D printers; CRISPR gene editing may facilitate the creation of biological weapons; cyber-physical systems offer new angles of attack.

- Syria offers an example of the intersecting vulnerabilities with cascading consequences that result from the collision of intrastate, interstate, and transnational tensions. Conflict between the government and rebel groups that began protesting during the Arab Spring became both a proxy war between the U.S., Russia, and a number of other nations, and a war against ISIS—creating 5.3 million refugees, and altering politics in the European Union.

- In Mexico, the government is facing another kind of threat: conflict between drug-related criminal organizations—and politicians, soldiers, law enforcement, and civilians—which has been responsible for between 80,000 and 100,000 deaths since 2006.

- On the other hand, there are states, such as China, which are using technologies to exert control, monitor social behavior, and reward that which conforms to the desires of the government.

- At the same time, China is focused intently on innovation and technology, and moving away from manufacturing, at a low-cost, products invented elsewhere. The role of education, research, and innovation is well established in creating economic and social power—and this is only likely to increase in the Fourth Industrial Revolution.

- Scientific and technological leadership is important for China's military power, but also for its claim to international political and economic leadership. A new order is beginning to appear. China now publishes nearly as many articles in peer-reviewed scientific and engineering journals as the United States.

- Under its 13th Five-Year Plan, China will increase public and private R&D spending from 2.1 percent to 2.5 percent of GDP—approaching the 2.8 percent the United States spends; raise the quality and volume of its patents; increase the contribution of scientific and technological advances to economic growth; and invest in human capital. By 2030, China and India together will supply 50% of the world's 25 to 34 year olds with tertiary education, and the U.S. just 8%.

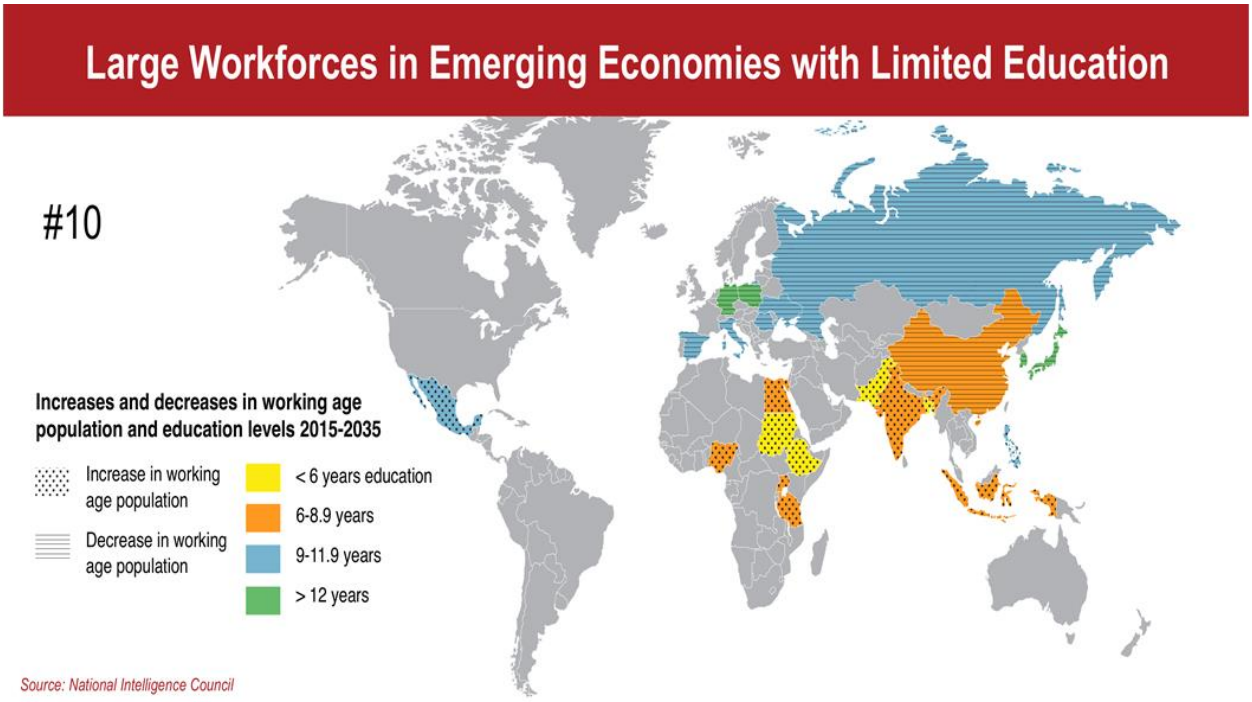
- Clearly, China is following a path to geopolitical leadership taken by the United States in the years following World War II—with government support for fundamental research and development, much of it conducted by universities, leading to the

breakthroughs that power industry. But when one considers China's stated priorities in science…it seems to be following Rensselaer Polytechnic Institute.

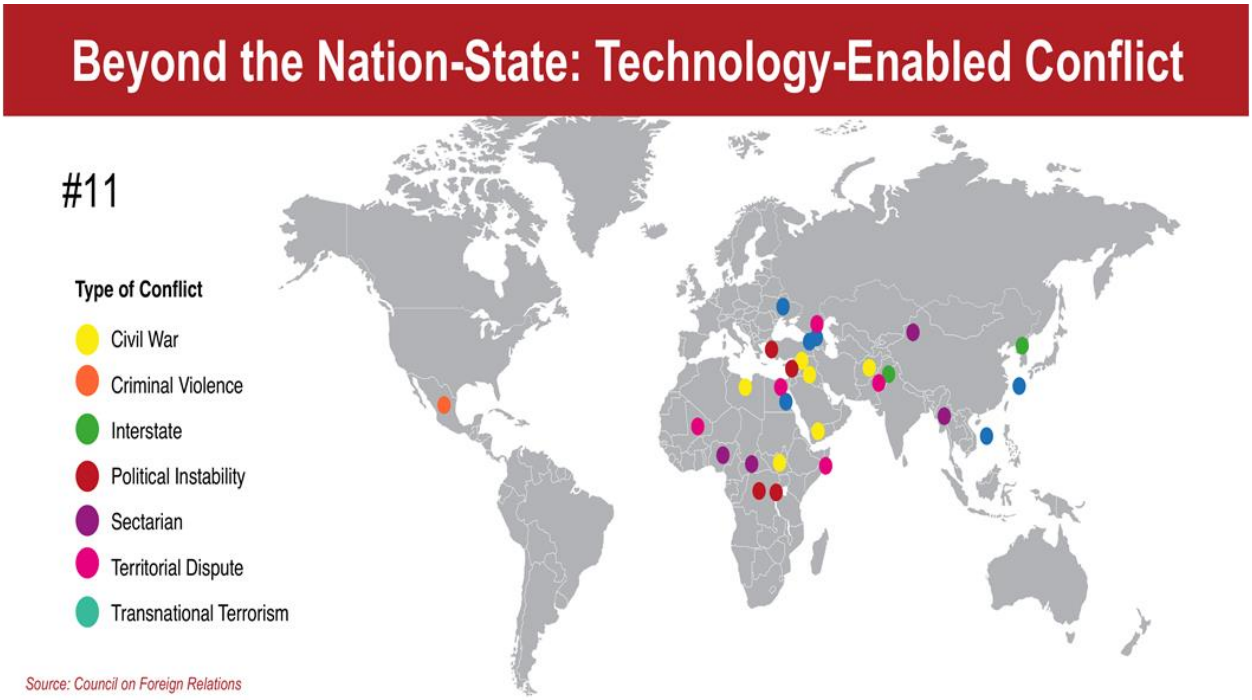
- These priorities include quantum communications and computing, brain research, cybersecurity, robotics, gene science, and big data applications—all strategic thrusts for Rensselaer as well.

- At Rensselaer, we believe that one of the linchpins of the Fourth Industrial Revolution will be an Intelligent Internet of Intelligent Things—in which the network is smart and recognizes opportunities and vulnerabilities in data streams—and the devices it connects also are smart, and able to adapt to changing conditions. This Intelligent Internet of Intelligent Things is crucial to addressing many challenges and opportunities, from cybersecurity, to advancing robotics, to enabling personalized medicine, to making use of the tsunami of digital data humanity is generating.

Education



Tech-enabled Conflict



- Geography is, to some extent, destiny—as is control of strategic resources. But the technologies of the Fourth Industrial Revolution will play strongly against emergent and historical geopolitical alignments.

- There will be a new energy equation, one in which more energy will be produced locally, as well as new definitions of critical strategic resources around the globe.

- Climate change will expose new vulnerabilities and new shocks to the global order—as well as reinforce the value of global coordination and cooperation.

- Demographics will force a new reckoning between the aging developed world and the youthful developing world.

- Technology will both allow transnational alliances—and deepen intrastate divisions.

- Together, these forces argue strongly for new mechanisms to promote peace and prosperity around the globe.

IV. Draft scenarios for GFC on the Future of International Security

The following three scenarios were drafted by GFC members and submitted for comment.

Scenario 1 Complexity

The Environment

The geopolitical environment of the early 2020s is one of intense competition between regional actors and great powers, particularly the United States and China in the Indo-Pacific.

In the Indo-Pacific, competition is accompanied by the dilution of long-standing alliance and partnership relationships. The U.S. hub-and-spoke alliance network is still operational in 2022. However, a gnawing and nearly axiomatic sense of uncertainty about U.S. commitment has settled in among Indo-Pacific partners after the 2016 election and 2018-2019 trade wars. Japan and Australia have begun hedging their geopolitical and military bets—not by drawing closer to China, but by developing capabilities and acting in ways independent of their partner relationships.

The competitive nature of the Indo-Pacific is mirrored in several domains of military activity. The cyber domain, electro-magnetic spectrum, undersea domain and missile versus missile defense are notable for the deterioration of American advantage globally and especially vis-à-vis China. China's successful testing in 2020 of a ship-borne electro-magnetic rail gun and in late 2021 of a maneuverable hypersonic glide vehicle—the ninth successful test of the Wu-14 / DZ/ZF during its development—introduced the prospect of these capabilities being operationally viable in the early-to-mid 2020s, ahead of estimates for the United States.

But it is in space where the risks of the burgeoning military-technological competition are most acutely felt as four powerful trends play out.

First, space in 2022 has less space, at least from low earth to geosynchronous orbit. More civilian government space agencies, militaries and intelligence communities, and even private companies are building new and enhanced constellations to reach the commercial and military 'commanding heights' of space. The lure of improved commercial communication and navigation, research and scientific capabilities, and military capabilities only gets stronger in the early 2020s.

Second, the competition in space is complex and multi-dimensional: getting there, denying others, building resilience, and enhancing capacity to operate without. The competition between denying space and building resilience grows especially intense from 2019 - 2022, moving well-beyond the crude mechanism of direct-ascent weapons designed to destroy satellites. Far more subtle means of denying the efficacy of commercial and military space assets—cyber-attacks, jamming or spoofing signals, dazzling or destroying satellites with lasers, using co-orbital

satellites to break space infrastructure—are assumed in 2022 to be part of the arsenals of the U.S., China, Russia, and, in some combination, other actors.

Third, impressive and cascading innovation in new technologies, including those associated with the 4th Industrial Revolution, are also at the core of space competition in the early 2020s. China's rapid ascent in quantum computing and encryption in the mid-and-late 2010s is shaping a global leading capability that has real and immediate implications for space in the early 2020s. China's ability to quantum encrypt communications to and from space—originally displayed in 2017 and subsequently enhanced in 2019—offers obvious advantage. Its successful development of quantum clocks in late 2020 was considered a stunning development, especially in Washington, that has rounded out China's capacity to operate absent the use of space-based assets, building an enhanced and still in 2022 un-replicated resilience.

Fourth, the development of both offensive and defensive space capabilities are outpacing the establishment of norms and regulations for their deployment and use. The space competition environment of 2022 increasingly reflects the dynamics that marked the undersea domain in the interwar period of the 20th century: Notionally, international law and norms prohibits militarization, but practically nations are developing capabilities in order to establish and maintain advantage the moment that geopolitical tension, uncertainty, and competition nearly inevitably spill over into this new domain; a prospect that portends not just to the erosion of advanced military capabilities, but to the destruction of infrastructure essential to modern states, societies and economies.

The Pathway

In the Spring of 2022, China's People Liberation Army Navy (PLAN) and Maritime Militia, after years of intermittent but increasingly regular and aggressive, shadowing of foreign ships, begin a weeks' long effort to harass foreign military ships transiting through the South China Sea as part of a broader approach to pursuing its maritime territorial claims in the area. In June of 2022, three Australian ships transiting from Subic Bay, Philippines to a port call in Vietnam are encountered by a robust PLAN force of surface ships and swarms of both unmanned aerial vehicles and unmanned surface vehicles. The episode concludes with a collision at sea between one Australian vessel and several unmanned surface vehicles. Several Australians are injured and two are killed as a result.

Anti-China protests are organized in major Australian cities, placing pressure on the government to respond in a forceful manner, though no immediately visible response is forthcoming.

Ten – days later, a U.S. destroyer collides with a Japanese shipping vessel near the Singapore Strait. A dozen Japanese nationals and six Americans are killed. Over three dozen combined are injured. China claims it is one more incident of poor U.S. Navy seamanship, but for the United States, there is clear and convincing evidence that the destroyer's navigation systems were hacked by a foreign actor. No official ties to the Chinese government can be definitely established, but the U.S. Intelligence Community is certain that China outsourced this attack to non-state actors.

Japan is livid at both China—for their presumed association with the attack—and the United States—for not being able to stop it. Domestic protests against both spread quickly across the country. Japan responds by launching its own cyber-attacks against China's social media and communications infrastructure with surprising success.

Public discourse in Japan and Australia questions whether the United States is still a reliable partner. Within the U.S. defense and national security community there is a strong impetus to act. Certainly, it must do something visible and in conjunction with its partners in order to demonstrate resolve and also contain what could be rapidly escalating crises between Japan / Australia and China.

The tempo and intensity of interactions on, beneath, and above the seas of the Western Pacific increases, leading to several more 'close calls'. Still, in the days after the tragic crash at sea, the Indo-Pacific command receives intelligence that China –using a combination of its Undersea Great Wall sensors and enhanced surface and undersea anti-submarine warfare capabilities-- has been able to identify and track Virginia – class subs in the South and East China, a development that hints at a rebalancing of the critical American (and allied) advantage in this domain.

The Pentagon also determines it must do something to signal China to slow down its risk-taking behaviour at a more strategic level and determines that the best means of doing this is by holding at risk China's now robust Beidou II global navigation satellite system and other space architecture. Attempts to hack and dazzle China's GPS-equivalent lead to responses in kind and to a deliberate, but still escalatory, competition in space to demonstrate exotic and difficult to attribute counter-space capabilities that plays out over several weeks in which there are conspicuous outages of both commercial and military communications and navigation infrastructure on both sides, with radiating consequences for those states linked into U.S. and Chinese GNSS and other space architecture.

The escalation in space is moving faster than the escalation on the seas and begins to take on a life of its own, reaching what appears to be a crescendo after approximately two months when China—seeking to dissuade further activity--blinds a U.S. nuclear early warning detection satellite, a red-line for U.S. defence planners. Two days later a failing U.S. commercial satellite nearly collides with a Beidou II satellite in GEO, leaving China to question whether this was a malicious or accidental event, further fuelling the potential for an even more radical and potentially kinetic escalation.

Scenario 2 Fragility

On a busy Friday, swarms of killer robots attack the world's largest stock exchanges in New York, London, and Tokyo simultaneously. The world is in shock. Dozens of employees are killed, the cities are in emergency state, and the financial system collapses.

Very quickly, Western governments, together with the companies affected, give press statements, explaining that the attacks must have been coordinated by Islamist terrorists. They announce a harsh response with military action.

Given the difficulties in attributing the attack to any specific perpetrator and the absence of a public statement by any major terrorist group, intellectuals and civil society organisations across Western countries warn from drawing premature conclusions and urge world leaders not to take military action until evidence is available. Cyber experts demonstrate that all major existing terrorist groups are unlikely to possess the capacity to coordinate such attacks successfully.

Nonetheless, Western leaders ensure the support by a critical mass of the population to engage in air strikes against several Middle Eastern countries, which are assumed to host the terrorist group accused of the attacks. Fake news of anti-Western letters claiming responsibility spread across social media. This makes leaders draw on an identity-based narrative to justify the airstrikes: they call upon their people to support them in defending Western values. When the airstrikes begin, the financial markets start to recover.

A few days into the airstrikes, government circles and the influential private sector companies obtain intelligence suggesting that the terrorist group accused of the attack had nothing to do with it. Instead, a transnational organised criminal (TOC) network was the perpetrator. The group staged the attack because they made money from betting against changes in the stock market. This group has been using information technologies to enhance benefits from the global illicit economy and had received support from government officials of certain “narco-states”. According to the documents that were circulated, the suspected officials seemed to stem from Guinea-Bissau, Mali, or Venezuela. While the international community had been focusing on high profile terrorist actors whose revenues stem to a large extend from the global illicit economy, this TOC group had kept a low profile and received little attention from international security and intelligence agencies. The TOC group has a loose network structure that spans the globe, it is not clear where their “headquarters” are located.

Despite robust evidence, the coalition of Western governments and business elites around the financial hubs withhold the information, the airstrikes continue. After the third week of airstrikes, a whistle-blower reveals the evidence about the TOC group to the public. Revelations are also made about the governments’ and the business elites’ knowledge of this at least two weeks earlier.

These revelations trigger anti-elite backlashes across the globe. Large protest movements form against governments and business elites, infuriated by the unnecessary loss of lives in the Middle Eastern countries due to the airstrikes. Government buildings and business centres in the US, UK and Japan are being vandalised, and Embassies are attacked by mobs. Meanwhile, some population groups still defend the initial narrative, claiming that the revelations are fake news. This leads to violent clashes between both sides, amplified by contradicting information spread on social media. Governments try to oppress the movements, with pictures of Western police forces brutally acting against protesters circulating in social media.

Guinea-Bissau, Mali, and Venezuela issued a joint statement, rejecting the recent accusations against them and called upon all countries from the Global South to support them in their defence against Western neo-imperialism. Populist movements across Latin America and Western Africa followed the call and start to protest. Venezuela stops selling oil to the US.

At an extraordinary Security Council meeting, Russia and China urge the US, UK, and France (supporting the US and the UK) to respect human rights, when taking measures against domestic protesters. They also call for the end of the airstrikes.

The airstrikes finally end, yet countless lives have been lost, the financial system is collapsed, and amidst the chaos, the global illicit economy is thriving, with criminal networks strengthening themselves across the globe and terrorist groups benefiting from deals with them to acquire cheap weapons, ammunitions and other resources needed to sustain attacks.

Scenario 3 Bio-economic warfare

In the third decade of the 21st century, great power relations were seeking ways to compete in terms of economic and technological supremacy in the context of the 4th Industrial Revolution, while maintaining access to a global economy on which their domestic political stability had become dependent. Two attempts to find a new medium of competition had failed. First, the use of conventional military force was frustrated by fear of escalation to a mutually destructive atomic war. Second, the trade wars of 2018-21 had ended expensively but indecisively, suggesting a similar futility on the economic level. The geopolitical challenge of the era was summed up by the question "how do you undermine your strategic adversary without jeopardizing your own prosperity or security?"

What happened next showed that there was a way to compete that got around the risk of economic or nuclear blowback, and it came to be known as "bio-economic warfare". The story unfolded as follows:

In the second decade of the 21st century, the US was gradually being pushed out of the Indo-Pacific by an assertive People`s Republic of China. Among the nations in the region who had relied on their alliances with the USA, some feared for their sovereignty and sought ways of deterring or degrading the threat from the PRC. All sought ways of distracting or degrading the strength of the PRC without provoking violent conflict (which all had come to believe they would lose). One of these states acquired from a non-state actor an engineered organism that had been developed to attack a strain of wheat that had come to produce the bulk of carbohydrates consumed in the PRC. The PRC had developed this genetically modified wheat to thrive in the polluted soils there, and to provide food security as it noticed it was increasingly dependent on imports from the Americas in the early 2000s. As a bio-agricultural project it was wildly successful. However, the homogeneity of the wheat strain represented a critical vulnerability in the food security sense, in that it was uniquely targetable in ways that restricted the damage to the "China strain" of wheat. None of the crops grown around the world would be affected, but it would throw the PRC`s food economy into a crisis, forcing it to rely on imports from the Americas, which retain the biggest global food export capacity. A widely-used fertilizer had been used as the transmission vehicle to spread the organism in a clandestine fashion. The hope was that the destruction of the China strain of wheat would be attributed to a natural disaster, rather than hostile action, and would thus not provoke retaliation.

Intelligence reports surfaced soon after via WikiLeaks, indicating that the organism that killed the "China strain" of wheat was developed in N. Korea as the bio-weapon of choice after it was disarmed by a joint US-China diplomatic coalition in 2021. A rival narrative quickly developed that this story had been put about merely to complicate the attribution of the attack. Either way, the debate bogged down at the United Nations Security Council, due to the lack of competence of an independent body that could evaluate competing claims and unresolved ambiguity as to whether it constituted a threat to international peace and security.

Another issue clouding the question of how to respond was that this approach to warfare was carefully configured to avoid causing direct human casualties. Unlike the earlier version of biological warfare (using disease to kill a defined enemy), this form of bio warfare was directed strictly at the adversary`s economic endowments. Much like what had happened in attempts to govern war in the cyber domain, it proved difficult to mobilize international action to govern bio-economic warfare because no-one got hurt or killed.

When Beijing learns of this bio-economic threat, it decides to dust off a plan to infect the US Navy with a superbug that corrodes the specific material used in sealing the pipes of the nuclear reactors that power its aircraft carrier fleet. The calculation is that this will throw the Sixth Fleet into crisis and cause US allies in the Western Pacific to exclude them from the region over safety concerns. In the end a few judiciously placed reports in blogs and newspapers in the region are enough to touch off a panic, and when the news management of the issue is mishandled by the Americans, the result is as successful as if an actual accident had occurred. A collective decision to exclude the US fleet from the Asian region is softened by dressing it up as an update of the original 1997 Southeast Asian Nuclear-Weapon-Free-Zone Treaty.

In an unintended consequence, The US National Security Council became alarmed that this superbug would spread to civilian nuclear plants in the homeland, and so decided to shut them down. Economic crisis follows, running down their defence capability.

The US then entered a national debate on how it could remain competitive with a 4th IR superpower China. Although some called for a declaration of war on China, this policy failed to gain any traction because no-one could explain how a strategy of “Cold War” style containment traditional war would put improve the situation of the US. Following the trend of the time, the US decides to retaliate with a superbug it has developed to attack the material used in the new type of semiconductors China developed in the period from 2019, when it was shut out of global investment opportunities in various 'strategic industries'. Like its China strain of wheat, the molecular make-up of the Chinese semiconductors was sufficiently specific to make them exclusively targetable in a way that minimised the risk of wider contamination. Once unleashed, this bug begins to cause extensive destruction in the Chinese economy and also among all those who purchased goods incorporating this type of semiconductor, including the Europeans. The US steps in to claim the global market on agricultural produce and semiconductors, enabling the temporary recovery of its economy.

However, the world as a whole is thrown back into economic recession under these conditions, and the growing number of states and non-state actors with relevant capability doubles down on bio engineering to wage successive waves of bio-economic warfare.