

Between Order and Chaos?

The Writing on the Wall

Strategic Monitor
2019-2020

Tim Sweijjs
Danny Pronk



Clingendael

Netherlands Institute of International Relations



Clingendael

Netherlands Institute of International Relations

Between Order and Chaos? The Writing on the Wall

Strategic Monitor 2019-2020

Tim Sweijs
Danny Pronk

January 2020

January 2020

© *The Hague* Centre for Strategic Studies

© Netherlands Institute of International Relations 'Clingendael'

Cover photo: © iStock

Contributors:

Marek Baron, Reinier Bergema, Esther Chavannes, Elisabeth Dick, Louk Faessen, Lucas Fagliano, Tara Görder, Goos Hofstee, Hugo van Manen, Minke Meijnders, Sico van der Meer, Juliette Schaffrath, Adája Stoetman, Bianca Torossian, Renske van der Veer, Koen van Wijk.

Reviewers:

Frank Bekkers, Ko Colijn, Monika Sie Dhian Ho, Rob de Wijk, Dick Zandee.

Unauthorised use of any materials violates copyright, trademark and / or other laws. Should a user download material from the website or any other source related to the *The Hague* Centre for Strategic Studies and/or the Netherlands Institute of International Relations 'Clingendael' for personal or non-commercial use, the user must retain all copyright, trademark or other similar notices contained in the original material or on any copies of this material.

Material on this website may be reproduced or publicly displayed, distributed or used for any public and non-commercial purposes, but only by mentioning the *The Hague* Centre for Strategic Studies and the Clingendael Institute as its source. Permission is required to use the logos of both organisations. This can be obtained by contacting the Communication desk of the Clingendael Institute (press@clingendael.org).




The following web link activities are prohibited by the Clingendael Institute and may present trademark and copyright infringement issues: links that involve unauthorised use of our logo, framing, inline links, or metatags, as well as hyperlinks or a form of link disguising the URL.

The Strategic Monitor 2019-2020 was commissioned by the Netherlands' ministries of Foreign Affairs and Defence within the PROGRESS framework agreement, Lot 5 (Strategic Monitoring & Foresight). Responsibility for the contents and for the opinions expressed rests solely with the authors. Publication does not constitute an endorsement by the Netherlands' ministries of Foreign Affairs and Defence.

HCSS

Lange Voorhout 1
2514 EA The Hague
The Netherlands

Follow us on social media:




-  @hcssnl
-  The Hague Centre for Strategic Studies
-  The Hague Centre for Strategic Studies

Email: info@hcss.nl
Website: www.hcss.nl

The Clingendael Institute

P.O. Box 93080
2509 AB The Hague
The Netherlands

Follow us on social media

-  @clingendaelorg
-  The Clingendael Institute
-  The Clingendael Institute

Email: info@clingendael.org
Website: www.clingendael.org

Note to readers

The Strategic Monitor 2019-2020 consists of this report, *Between Order and Chaos? The Writing on the Wall*, and ten individual studies that are available online.

Please see www.hcss.nl/monitor and www.clingendael.org/monitor.

Contents

Executive summary	1
Samenvatting	5
1 Introduction	9
2 Development of the Threat	16
2.1 Military Competition	16
2.2 Cyber Security	22
2.3 Hybrid Conflict	27
2.4 Economic Security	36
2.5 CBRN Weapons	41
2.6 Terrorism	43
2.7 Sub-conclusions	47
3 Development of the International Order	49
3.1 Military Competition	49
3.2 Cyber Security	58
3.3 Hybrid Conflict	64
3.4 Economic Security	68
3.5 CBRN Weapons	71
3.6 Terrorism	75
3.7 Sub-conclusions	78
4 Geodynamics	80
4.1 Socio-economic	82
4.2 Connectedness	85
4.3 Identity	87
4.4 Political	90
4.5 Judicial	93
4.6 Security	96
4.7 Sub-conclusions	98

5	The Netherlands in the World	100
5.1	The Netherlands and Foreign Relations	104
5.2	Which States are the Most Relevant?	108
5.3	Which States are the Most Compatible?	111
5.4	Sub-conclusions	114
6	Security is in the Eye of the Beholder	116
6.1	On the Role of Biases in Perceptions	116
6.2	International Security Perceptions	119
6.3	Sub-conclusions	127
7	Conclusion	128
8	Bibliography	137

Executive summary

This Strategic Monitor 2019-2020, *Between Order and Chaos? The Writing on the Wall*, examines the structural long-term trends and current events that shape the global security environment and that influence Dutch national interests and values. This year's report looks in more detail at the emergence of a new world order, or rather, orders. The report describes and analyzes the most important developments in the international regimes that form the international order. In seven chapters the trends and developments in international relations and the Dutch security environment are studied and interpreted, taking stock of the world today and tomorrow.

This Strategic Monitor examines the trends and developments with regard to the six most urgent security threats from *Worldwide for a safe Netherlands: Integrated Foreign and Security Strategy 2018-2022*: military threats, cyber threats, unwanted foreign interference and undermining, threats to vital economic processes, the threat of chemical, biological, radiological and nuclear (CBRN) weapons, and terrorist attacks. Most indicators for these six themes point to an increased threat for the coming five years. The trends and developments in the international order reveal a predominantly negative picture with regard to four themes: military competition, hybrid conflict, economic security, and CBRN weapons. For all four of these themes, the degree of cooperation in the international order is shifting towards a greater struggle over the norms and rules of the existing regimes. Trends and developments related to new rules development in cyberspace and rules compliance in counterterrorism are, however, decidedly more positive in nature. Here we see the development of new standards in cyberspace and increasing cooperation in the international efforts to combat terrorism.

Our analysis of global geodynamics yields a kaleidoscopic picture. The world population has become more prosperous, but inequality has also increased by different measures. Although the world as a whole continues to become more connected, increased connectivity has not necessarily brought people closer together. Societies worldwide have not become more inclusionary, due to a marked increase in identity-driven politics, higher levels of religious restrictiveness, and increases in social hostilities. At the same time, the rule of law has been strengthened and, despite the structural human rights violations in a number of countries, research suggests that human rights protection regimes are improving over time. But despite the growth and spread of democracy over the past two decades, democracy as an institution and especially individual freedoms are under prolonged attack. Civil and political rights have been declining for over a decade now, in both free and unfree countries. At the same time, illiberal governments have undeniably been gaining more influence in the

regulation of global affairs. Finally, over the past two decades, the world has become less peaceful and secure because of a growing number of conflicts and conflict fatalities.

On the world stage, the Netherlands finds itself in a relatively fortunate position. It can count on close allies and partners in its immediate geographic surroundings. Despite ongoing turbulence in the European Union, this regional regime is becoming more relevant for the Netherlands. While the United States and Germany continue to be dominant in Dutch foreign relations, emerging powers have become more relevant as measured along economic, political, and military dimensions over the past decade. China's ascent economically, militarily, and politically, in combination with the fact that China has a different values system than the Netherlands, implies that, for the Netherlands, China presents both an opportunity and a risk. In addition, a number of middle powers have both become more relevant and moved closer to the Netherlands on important value dimensions, which means that the Netherlands has a range of potential partners to collaborate with in shaping international regimes and rules in this changing context.

Interestingly, a number of other countries in their international security documents not only have a different assessment of the six threats identified in the *Integrated Foreign and Security Strategy 2018-2022*, but also give greater weight to additional threats. These include climate change and the exploitation and militarization of space. However, as in the Dutch case, most of these documents pay very little attention to the other side of the security coin: opportunities. It is recommended that these two observations be taken into consideration in the design of next year's activities in the framework of the Strategic Monitor.

Overall, this Strategic Monitor concludes that the tenets of the international order continue to shift. Here it is important to recognize that it is the combination of national and international vectors that converge to undermine bastions of the existing international order, both from within and from without, both bottom-up and top-down.

Increased global competition across military, economic, and political domains goes hand in hand with a persistent erosion of significant aspects of the existing architecture of the international order. Compliance and cooperation are giving way to violation and confrontation across important political, economic, and security regimes, and rules are systematically violated while underlying norms are incrementally hollowed out. There are, however, certainly areas in which international cooperation persists, albeit in the context of voluntary and non-binding initiatives of coalitions of the willing, comprising both national and local governments, and increasingly in partnership with non-state and private actors. The shifts described in this report all take place in an era of rapid technological change, generating a host of new challenges to political and societal cohesion, economic equality, national security, and fundamental human rights.

The increased global competition is having important implications for the nature of threats, including the further fusion of the internal-external security nexus. Borders, physical or otherwise, no longer shield against the dangers posed by external forces. This implies the compression of time and geographical distance. Increased competition is also accompanied by the spillover of threats from one domain to another, with multidomain threats becoming the rule rather than the exception in the context of a connected world.

The dynamics of the US-Sino rivalry will be different from those between the US and the Soviet Union during the Cold War: the former will take place across multiple domains in the context of a more tightly integrated global economy. Some degree of economic protectionism can be expected to remain part of future US policies, alongside a continued strategy of military pre-eminence. Interdependence in different domains can contribute to stability by creating mutual interests, but it can also contribute to the spillover effects that fuel negative spiral dynamics. Economic decoupling into different blocs around the US and China will remove incentives to constrain competition in other domains, most importantly the military domain.

Now, do these developments signify the demise of the existing international order, or do they merely represent a perhaps overdue renovation of regimes within that order that are no longer fit for purpose? The developments suggest a little bit of both: some elements in the existing international order are revised and brought in sync with the global distribution of power; other elements are redesigned from scratch. This leaves the shape of the emerging international order still uncertain, but not entirely unclear during this period of transition.

Based on this year's reading of the writing on the wall, international relations are expected to feature more outright forms of competition in the economic, military, but also in the ideological realm. The international order is expected to become less liberal in nature and less global in scope, and it will be more fragmented. However, modern means of communication and transportation will continue to facilitate coordination and collaboration that underpin the regimes that make up the order, and vested interests, both public and private, will continue to argue for international coordination and collaboration. Despite ideological differences and competing interests, the urgency of various key international challenges, such as climate change or nuclear proliferation, may yield sufficient pressure on global political leaders to act.

What does this outlook mean for the Netherlands? In light of increasing competition in the context of a decaying order, lopsided dependence on single actors across multiple fields is potentially dangerous. Investing in greater strategic autonomy, not just militarily but also economically and politically, creates greater maneuvering room, which in turn contributes not only to the security and prosperity of the Netherlands but also to the stability of the system at large. Strong collaboration within Europe will remain

indispensable, not as an end in itself but as an instrument. However, the changing context and the adaptation of the existing order require greater investment in bilateral relationships that can help achieve Dutch core interests, both inside and outside of multilateral frameworks. In selecting such partnerships and making strategic choices, it is vital to have a clear understanding of the vulnerabilities to which the Netherlands is exposed as well as of the opportunities which the Netherlands can leverage.

The changing context requires not just new partnerships, but also concept development and experimentation with new strategies to keep up with the evolving foreign policy environment. Finally, the changing international context does not mean that we should ignore or under-appreciate our own values. It rather means the opposite. Increasing rivalry between values systems in the world requires that we also make more explicit what we stand for, and which way of life we want to protect and develop, and that where possible we actively use our values as an instrument of power and influence.

Samenvatting

Deze Strategische Monitor 2019-2020, *Tussen orde en chaos? De tekenen aan de wand*, onderzoekt de structurele lange-termijntrends en actuele gebeurtenissen die de mondiale veiligheidsomgeving vormen en van invloed zijn op de Nederlandse nationale belangen en waarden. Het rapport van dit jaar gaat dieper in op het ontstaan van een nieuwe wereldorde, of beter gezegd, ordes. Het rapport beschrijft en analyseert de belangrijkste veranderingen in de internationale regimes die de internationale orde vormen. In zeven hoofdstukken worden de trends en ontwikkelingen in de internationale betrekkingen en in de veiligheidsomgeving van Nederland onderzocht en geïnterpreteerd, en wordt de balans opgemaakt van de wereld van vandaag en morgen.

In deze Strategische Monitor worden de trends en ontwikkelingen onderzocht ten aanzien van de zes meest urgente veiligheidsbedreigingen uit *Wereldwijd voor een veilig Nederland: Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022*, te weten militaire dreigingen, cyberdreigingen, ongewenste buitenlandse inmenging en ondermijning, bedreiging van vitale economische processen, dreiging van chemische, biologische, radiologische en nucleaire (CBRN) middelen en terroristische aanslagen. De meeste indicatoren voor deze zes thema's wijzen op een verhoogde dreiging voor de komende vijf jaar. De trends en ontwikkelingen in de internationale orde geven een negatief beeld met betrekking tot vier thema's: militaire competitie, hybride conflicten, economische veiligheid en CBRN-wapens. Voor alle vier deze thema's verschuift de mate van samenwerking in de internationale orde naar meer strijd over de normen en regels van de bestaande regimes. De trends en ontwikkelingen met betrekking tot nieuwe normontwikkeling in cyberspace en normconformiteit bij terrorismebestrijding zijn echter beslist positiever van aard. Hier zien we de ontwikkeling van nieuwe normen in cyberspace en meer samenwerking bij internationale inspanningen op het gebied van terrorismebestrijding.

Onze analyse van de mondiale geodynamiek levert een caleidoscopisch beeld op. De wereldbevolking als geheel is welvarender geworden, maar ook de ongelijkheid is toegenomen. En ondanks dat de wereld als geheel meer verbonden raakt, heeft de verhoogde connectiviteit de mensen niet per se dichter bij elkaar gebracht. Wereldwijd zijn samenlevingen minder inclusief geworden door een toename van identiteit-gedreven politiek, een groter aantal religieuze beperkingen en een toename van maatschappelijke polarisatie. Tegelijkertijd is de rechtsstaat versterkt en suggereert onderzoek dat de bescherming van de mensenrechten, ondanks stelselmatige mensenrechtenschendingen in een aantal landen, in de loop van de tijd verbetert. Maar ondanks de groei en verspreiding van democratie in de afgelopen twee decennia, staat democratie als zodanig, en met name individuele vrijheden, onder druk. Politieke rechten en burgerlijke

vrijheden nemen nu al meer dan tien jaar af, zowel in vrije als in minder vrije landen. Tegelijkertijd hebben onliberale staten ontegenzeggelijk meer invloed gekregen in de regulering van mondiale aangelegenheden. Ten slotte is de wereld de afgelopen twee decennia minder vredig en veilig geworden.

Nederland bevindt zich op het wereldtoneel in een relatief gelukkige positie. Het kan rekenen op bondgenoten en partners in zijn directe geografische omgeving. En ondanks aanhoudende turbulentie in de Europese Unie wordt dit regionale regime steeds relevanter voor Nederland. Terwijl de Verenigde Staten en Duitsland dominant blijven in de Nederlandse buitenlandse betrekkingen, zijn opkomende mogendheden, gemeten langs de economische, politieke en militaire dimensies, in het afgelopen decennium relevanter geworden. China's economische, militaire en politieke opkomst, in combinatie met het feit dat het land een ander waardensysteem kent dan Nederland, betekent dat China voor Nederland zowel een kans als een bedreiging is. Daarnaast is een aantal midden-machten relevanter geworden en op waardenniveau dichter bij Nederland gekomen, hetgeen betekent dat Nederland een scala aan potentiële partners heeft om mee samen te werken bij het vormgeven van internationale regimes en regelgeving in deze veranderende mondiale context.

Interessant is dat een aantal andere landen in hun internationale veiligheidsdocumenten niet alleen de zes bedreigingen uit de *Geïntegreerde Buitenland- en Veiligheidsstrategie 2018-2022* verschillend beoordelen, maar ook meer gewicht toekennen aan andere bedreigingen. Deze omvatten klimaatverandering en de exploitatie en militarisering van de ruimte. Net als in het Nederlandse geval wordt in het buitenlandse veiligheidsdiscours weinig aandacht besteed aan de andere kant van de medaille: de kansen. Aanbevolen wordt om met deze twee observaties rekening te houden bij het ontwerp van de activiteiten van het volgende jaar in het kader van de Strategische Monitor.

Over het geheel genomen concludeert deze Strategische Monitor dat de kaders van de internationale orde blijven verschuiven. Hierbij is het belangrijk te onderkennen dat het de combinatie is van nationale en internationale vectoren die samenkomen om de bastions van de bestaande internationale orde te ondermijnen, zowel van binnenuit als van buitenaf, zowel *bottom-up* als *top-down*.

Toenemende wereldwijde concurrentie in de militaire, economische en politieke domeinen gaat hand in hand met een aanhoudende erosie van belangrijke aspecten van de bestaande architectuur van de internationale orde. Naleving en samenwerking maken plaats voor schending en confrontatie in belangrijke politieke, economische en veiligheidsregimes, en regels worden systematisch overtreden terwijl de onderliggende normen geleidelijk worden uitgehold. Er zijn echter ook gebieden waarop de internationale samenwerking stand houdt, zij het vaker in de context van vrijwillige en niet-bindende initiatieven van gelegenheidscoalities, bestaande uit zowel nationale als

lokale overheden, en in toenemende mate in samenwerking met niet-statelijke en private actoren. De verschuivingen die in dit rapport worden beschreven, vinden bovendien allemaal plaats in een tijdperk van snelle technologische veranderingen, die een groot aantal nieuwe uitdagingen met zich meebrengen voor politieke en maatschappelijke cohesie, economische gelijkheid, nationale veiligheid en fundamentele mensenrechten.

De toegenomen wereldwijde concurrentie heeft ook belangrijke implicaties voor de aard van de bedreigingen, waaronder de verdergaande samensmelting van de interne en externe veiligheidsdimensies. Grenzen, fysiek of anderszins, beschermen niet langer tegen de gevaren van externe krachten. Dit impliceert een compressie van tijd en geografische afstand. Méér concurrentie gaat ook gepaard met spillover van bedreigingen van het ene domein naar het andere, waarbij multi-domeinbedreigingen zoals hybride conflictvoering eerder de regel dan uitzondering worden in de context van een verbonden wereld.

De dynamiek van de rivaliteit tussen de VS en China zal anders zijn dan die tussen de VS en de Sovjet-Unie tijdens de Koude Oorlog. Eerstgenoemde zal plaatsvinden over verscheidene domeinen in de context van een veel nauwer geïntegreerde mondiale economie. Van het toekomstige Amerikaanse beleid wordt verwacht dat dit gekenmerkt zal worden door een zekere mate van economisch protectionisme, naast een strategie gericht op het behoud van de militaire dominantie. Onderlinge afhankelijkheid in verschillende domeinen kan weliswaar bijdragen aan stabiliteit, maar het kan ook bijdragen aan de spillovereffecten die een negatieve spiraaldynamiek voeden. Economische ont koppeling in gescheiden blokken aangevoerd door respectievelijk de VS en China zal de prikkels om concurrentie op andere domeinen te beperken, vooral het militaire, wegnemen.

Betekenen deze ontwikkelingen nu de ondergang van de bestaande internationale orde, of vertegenwoordigen ze slechts een renovatie van die regimes binnen de orde die niet langer bij de tijd zijn? De ontwikkelingen suggereren dat het een beetje van beide is: sommige elementen van de bestaande orde worden herzien en gesynchroniseerd met veranderingen in de mondiale machtsverdeling, andere elementen worden helemaal opnieuw ontworpen. Daarmee is tijdens deze overgangperiode de vorm die de internationale orde gaat aannemen nog steeds onzeker, maar niet helemaal onduidelijk.

Op basis van onze analyse van de tekenen aan de wand, verwachten wij dat de internationale betrekkingen meer openlijke vormen van concurrentie zullen vertonen in de economische, militaire, maar ook in de ideologische sfeer. De internationale orde zal naar verwachting minder liberaal en minder mondiaal van aard worden en zal meer gefragmenteerd zijn. Maar moderne telecommunicatie- en transportmiddelen zullen de coördinatie en samenwerking blijven ondersteunen die ten grondslag liggen aan de bestaande regimes, en actoren, zowel publieke als private, zullen blijven pleiten voor internationale coördinatie en samenwerking. Ondanks ideologische verschillen en

tegengestelde belangen, kan de urgentie van verschillende belangrijke internationale uitdagingen, zoals klimaatverandering of nucleaire proliferatie, leiden tot voldoende druk op politieke leiders om op te treden.

Wat betekent dit vooruitzicht voor Nederland? In het licht van de toenemende concurrentie in de context van een veranderende internationale orde is eenzijdige afhankelijkheid van bepaalde actoren potentieel gevaarlijk. Investeren in een grotere strategische autonomie, niet alleen militair, maar ook economisch en politiek, creëert een grotere manoeuvreerruimte, die op zijn beurt niet alleen bijdraagt aan de veiligheid en welvaart van Nederland, maar ook aan de stabiliteit van het mondiale systeem als geheel. Sterke samenwerking binnen Europa blijft daarbij onmisbaar, niet als doel op zich, maar als instrument. De veranderende context en de aanpassing van de bestaande orde vereisen meer investeringen in bilaterale betrekkingen die kunnen helpen Nederlandse belangen te behartigen, zowel binnen als buiten multilaterale kaders. Bij het selecteren van dergelijke partnerschappen en het maken van strategische keuzes is het van vitaal belang om een goed begrip te hebben van de bedreigingen waaraan Nederland is blootgesteld, evenals van de kansen die Nederland kan benutten.

De veranderende mondiale context vereist niet alleen nieuwe partnerschappen, maar ook de ontwikkeling van en experimenten met nieuwe concepten en strategieën om gelijke tred te houden met de veranderende omgeving van het buitenlands beleid. Tenslotte betekent de veranderende internationale context niet dat we onze eigen waarden moeten veronachtzamen. Het betekent eerder het tegenovergestelde. De toenemende rivaliteit tussen waardensystemen in de wereld vereist dat wij ook expliciteren waar wij voor staan, wat wij willen beschermen en willen bevorderen, en dat wij waar mogelijk onze waarden actief inzetten als een instrument van macht en invloed.

1 Introduction

This report focuses on long-term structural developments as well as current events that shape the global security environment and affect Dutch national interests and values. The title of this year's Strategic Monitor, *Between Order and Chaos? The Writing on the Wall*, is a reference to the warning of impending discontinuity in the biblical tale of Belshazzar, king of Babylon, as described in the book of Daniel. Belshazzar hosted a lavish feast for more than a thousand dignitaries for which he had used gold and silver goblets taken from the temple in Jerusalem. These goblets were sacred, but the king and his guests drank from them anyway. During the feast a hand appeared and wrote an inscription on a wall. The terrified king called on his magicians to explain what the writing on the wall meant. Only Daniel, the head of the king's seers, could decipher it. Daniel explained that the writing was a warning to Belshazzar that his days as king were numbered because of his arrogance toward God, and that his kingdom would be split in two. Sudden, structural change such as the end of Belshazzar's kingdom is a key feature of discontinuity. And the challenge for strategic analysts is to decipher the writing on the wall and to foresee possible future events and developments.

The annual Strategic Monitors have been taking stock of events and developments for almost a decade now. Born out of the Dutch interdepartmental *Defense Policy Survey* of 2010, the continuous Strategic Monitor horizon-scanning efforts contribute to the government's long-term strategic anticipation function.¹ In previous iterations, they identified and warned about spikes in great power assertiveness (2013-2014), the risks of conflict breaking out over pivot states (2014), the fragility of the Middle East and the contagious effects of political violence (2014 and 2017), the return of interstate crisis in hybrid guises (2014-2015), and the emergence of a multi-order (2017). In last year's report, we identified the existence of an interregnum, a transition phase during which the old had died but the new was yet to be born (2018).²

This year, we delve deeper into the development of a new international order, or, more precisely, orders. We conceive of the international order not just from the perspective of a liberal world order, but look at it more broadly as being rooted in a collection of international regimes, which are defined as "a set of implicit and explicit principles, norms, rules and decision-making procedures around which the actors converge in

1 "Verkenningen Houvast Voor de Krijgsmacht van de Toekomst" (Ministerie van Defensie, 2010).

2 Tim Sweijts and Danny Pronk, "Interregnum | Strategic Monitor 2018-2019" (HCSS, 2018).

a particular area of international relations.”³ Orders can be global or regional, and they can be ideological (for instance, liberal) or agnostic in nature.⁴ The post-Second World War international liberal order, for instance, never encompassed all countries. Certainly during the Cold War period it was a regional order, rather than a global one, except at the very top with the United Nations. Similarly, these orders can be thin or thick in nature: thin orders feature selective elements of engagement on a limited number of important issues (e.g., state sovereignty and arms control); thick orders are characterized by norms and rules that suffuse many aspects of international relations (e.g., trade, human rights, the environment, etc.). The latter is visible in the liberal order that was constructed after the Second World War, came of age during the Cold War, matured further in the 1990s and the 2000s and is now under severe pressure.⁵ Orders are rooted in a distribution of power that gives “rise to a relatively stable pattern of relationships and behaviors.”⁶ These stable patterns are then institutionalized in the form of coordination arrangements and regimes that are considered legitimate by the most important actors. Orders therefore rest on power and legitimacy.⁷

In times of rapid shifts in the international distribution of power, these stable patterns are undercut by the foreign policy of states dissatisfied with the status quo and with their roles in the system. These states start contesting the role of the leading state, aspiring to a more dominant role in the regulation of international affairs for themselves. This process leads to increased international competition, not just in a narrow, traditional geopolitical sense, but understood more broadly as ‘the attempt to gain advantage, often relative to others believed to pose a challenge or threat, through the self-interested pursuit of contested goods such as power, security, wealth, influence, and status.’⁸ Dissatisfaction thus breeds increased competition, which in turn seriously undermines

3 Stephen Krasner, “Structural Causes and Regime Consequences: Regimes as Intervening Variables,” *International Organization*, 1982.

4 For the distinction, see John J. Mearsheimer, “Bound to Fail: The Rise and Fall of the Liberal International Order,” *International Security* 43, no. 4 (April 1, 2019): 7–50.

5 For different aspects of the liberal order, see John Ikenberry, “The End of Liberal International Order?,” *International Affairs* 94, no. 1 (January 1, 2018): 7–23.

6 Andrew Heywood, *Political Theory: An Introduction* (Macmillan International Higher Education, 2015), 339.

7 Henry Kissinger, *World Order*, 2014.

8 Michael J. Mazarr et al., *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives* (RAND Corporation, 2018). We thus conceive of competition within a much broader perspective than a traditional geopolitical perspective which defines geopolitics as the interplay among geography, power, politics, and international relations on the Earth’s surface.

existing regimes and upsets the existing dominant order. It also leads to friction and to crisis and sometimes to conflict and can even escalate to war between contenders and defenders of the status quo.⁹

With the benefit of hindsight, dissatisfaction has been lurking not only under, but also at the surface for quite some time now. For instance, in his 2007 Munich Security Conference speech, Russia's President Vladimir Putin openly declared that "the unipolar model is not only unacceptable, but also impossible in today's world."¹⁰ President Putin denounced "unilateral and frequently illegitimate actions" and asserted that "the United States has overstepped its national borders in every way" because of "the economic, political, cultural, and educational policies it imposes on other nations." Observing that "the economic potential of the new centers of global economic growth will inevitably be converted into political influence and will strengthen multi-polarity," he called for a serious rethink of "the architecture of global security" and "a reasonable balance between the interests of all participants in the international dialogue." Vladimir Putin was not alone in uttering these sentiments. Less antagonistically, but equally determined, China's President Xi Jinping laid out in 2013 his goal of pursuing "a renaissance of the Chinese nation,"¹¹ calling for a "new type of major power relations" and, more recently, "a new form of international relations featuring mutual respect, fairness, justice, and win-win cooperation."¹² Now, as we are entering the third decade of the twenty-first century, European leaders can no longer ignore the impacts of both international and domestic developments on the sustainability of rules and regulations of the international order. At the end of 2019, Emmanuel Macron declared a moment of "unprecedented crisis in our international system," which "requires new alliances and new ways to cooperate."¹³ And even though the French president views a stronger Europe in many

9 For the logic, see Charles F. Doran, "Economics, Philosophy of History, and the 'Single Dynamic' of Power Cycle Theory: Expectations, Competition, and Statecraft," *International Political Science Review* 24, no. 1 (January 1, 2003): 13–49. For the argument that it leads to war, see Graham Allison, the Thucydides Trap. Without going into the whole power transition debate, for a list of works that argue otherwise, a good place to start is Lebow, see Richard Ned Lebow and Benjamin Valentino, "Lost in Transition: A Critical Analysis of Power Transition Theory," *International Relations* 23, no. 3 (September 1, 2009): 389–410.

10 "Speech and the Following Discussion at the Munich Conference on Security Policy," Office of the President, November 29, 2019.

11 "Xi Jinping Outlines His Vision of 'Dream and Renaissance,'" *South China Morning Post*, March 18, 2013.

12 See-Won Byun, "China's Major-Powers Discourse in the Xi Jinping Era: Tragedy of Great Power Politics Revisited?," *Asian Perspective* 40, no. 3 (2016): 493–522. For a more recent speech in which Xi Jinping laid out his vision, see Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," *Qiushi Journal*, accessed December 9, 2019.

13 "Emmanuel Macron in His Own Words (English)," *The Economist*, November 26, 2016.

respects as a necessary precondition to transcend this crisis, Macron considers our continent to be “on the edge of a precipice,” with growing societal polarization, considerable disparities between West and East, and a seemingly never-ending Brexit.¹⁴

The Strategic Monitor annual report monitors, describes, and analyzes the ongoing transition and assesses changes across international regimes that are important tenets of the current international order.¹⁵ The outcome of this transition is far from certain, but it is clear that current events have significant ramifications for the future of international relations, including the rules and regulations guiding state interaction. The international order can evolve in multiple directions at the same time, across different domains of state interaction: it can incline more toward international cooperation, as it would in an ideal notion of a liberal international democratic order, but in parallel it can also evolve toward more international competition. Because of path dependency, developments in the early stages of international order formation have disproportional effects on later outcomes or phases of the order.¹⁶ A better understanding of developments will help policymakers to ‘get there early’ and provide a basis for informed action.¹⁷

In this context, this report investigates and interprets the developments in international relations and in our security environment, and answers the following question: *What have been the main developments in the past ten years with regard to international security, and what trends are in prospect for the next five years?* In the following six chapters, we take stock of the world of today and of tomorrow. Chapter 2 looks at trends and developments with regard to the six most urgent security threats from the Dutch policy white paper *Worldwide for a safe Netherlands: Integrated Foreign and Security Strategy 2018–2022*: military threats, cyber threats, unwanted foreign interference and undermining, threats to vital economic processes, the threat of chemical, biological, radiological and nuclear (CBRN) weapons, and terrorist attacks, and assesses their impact on Dutch national security interests. Chapter 3 examines trends and developments in international regimes based on these same six themes. Chapter 4 turns to geodynamics in the global system and considers structural trends in socio-economic, identity, connectedness, judicial, political, and security domains, in order to provide a snapshot of the state of humanity at multiple levels.¹⁸ Chapter 5 surveys the role and the position of the Netherlands in the world based on an empirical analysis of Dutch foreign relations in the political, economic, security, and human rights realm. Chapter 6 explores

14 Wintour Patrick, “Nato to Consider Expert Panel after Macron Brain-Dead Claim,” *The Guardian*, November 26, 2019.

15 Tim Sweijts and Danny Pronk, “Interregnum: Strategic Monitor Annual Report 2019” (The Hague, Netherlands: The Hague Centre for Strategic Studies & The Clingendael Institute, April 2019).

16 Paul Pierson, *Politics in Time: History, Institutions, and Social Analysis* (Princeton University Press, 2011).

17 Bob Johansen, *Get There Early: Sensing the Future to Compete in the Present*, 2007.

18 Julian L. Simon, *The State of Humanity*, 1996.

global perspectives of important third actors on the six threat themes and identifies differences and similarities. Chapter 7 draws conclusions regarding the threats and international regimes, dominant geodynamics, and the role of the Netherlands. This in turn feeds into an overall assessment of the evolving international order in this period of transition.

The research activities conducted for this year’s Strategic Monitor led to the publication of ten individual in-depth studies in various sub-areas.¹⁹ This report provides an overall framework with which to understand the results of these individual studies (which are of value in their own right) in a more comprehensive context (see Table 1). The ten in-depth studies provide further background, data, analysis, as well as references to the literature used. They thus provide the body of evidence for the insights that are provided here in a more concise form.

Table 1 List of the ten in-depth studies undertaken as part of this Strategic Monitor

<i>Military Competition in Perspective: Trends in Major Powers’ Postures and Perceptions</i>
<i>Cyber security: Parsing the Threats and the State of International Order</i>
<i>Hybrid Conflict: Neither War nor Peace</i>
<i>Economic Security with Chinese Characteristics</i>
<i>CBRN Weapons: Where Are We in Averting Armageddon?</i>
<i>Terrorism in the Age of Technology</i>
<i>What World Do We Live In? An Analysis of Geodynamic Trends</i>
<i>The Evolving Position of the Netherlands in the World</i>
<i>In the Eye of the Beholder? An Assessment of Global Security Perceptions</i>
<i>Perceptions of Security: How Our Brains Can Fool Us</i>

To answer the central research question, a wide range of methods and techniques were used to assess the current and future security environment from different analytical perspectives.²⁰

19 These in-depth studies are publicly available on the two online platforms of Clingendael and HCSS: <https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/> and <https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/>.

20 These methods and techniques were described in greater detail in our research paper *Analyzing the Future, Our Methodology*. For this see: “Strategic Monitor 2018–2019,” accessed December 9, 2019.

Threat assessment (chapter 2). To analyze the threats, a horizon-scanning method was used, involving a structured investigation of the six threat themes in the literature from government, international organizations, think tanks, and academia, supplemented with information from media and social media. Expressed in a set of indicators for each of the investigated themes, the developments over the last ten years were assessed and further validated using expert judgment. These sets of indicators then served as a basis for making statements on the trends expected over the next five years (up to 2025). Finally, the findings on the threats were linked to the Dutch national security interests to see whether and to what extent they are actually threatened. The Strategic Monitor considers three core interests: 1) national legal order and public security; 2) international legal order; and 3) economic prosperity. These three interests are derived from those used by the various ministries and are consistent with the Constitution, the Charter for the Kingdom of the Netherlands, and further Dutch legal obligations.²¹ In the six respective trend tables in chapter 2, upward trends are indicated with ▲, downward trends with ▼, and stable trends with ▬. These trends are further qualified as being either positive (■) or negative (■) in character, based on their impact on the three Dutch national security interests.

International cooperation and conflict (chapter 3). A comparative approach was used to gauge shifts in the degree of cooperation in the international regimes that together make up an international order for each of the six investigated themes.²² For each regime, an analysis was made of the extent to which states comply with concrete rules and agreements within the relevant regimes, and with the underlying norms on which those rules and agreements are based.²³ In the six respective trend tables in chapter 3, upward trends are again indicated with ▲, downward trends with ▼, and stable trends with ▬. These trends are again further qualified as being either positive (■) or negative (■) in character, based on their impact on the international order encapsulated in these various regimes.

Geodynamics (chapter 4). Next, this report assesses structural developments using a multi-perspective approach. It analyzes an assortment of developments across the socio-economic, identity, connectedness, judicial, political, and security domains at the level of the individual, the state, and the international order. In the six respective trend tables in chapter 4, upward trends are again indicated with ▲, downward trends

21 Kars De Bruijne, "Vitale Belangen" (Clingendael, 2018).

22 See Krasner, Stephen Krasner, "Structural Causes and Regime Consequences: Regimes as Intervening Variables."

23 These world views were originally developed as scenarios for and presented in "Verkenningen Houvast Voor de Krijgsmacht van de Toekomst." and since then they have been used as a constant reference framework in the previous eight editions of the Strategic Monitor (2012 to 2019).

with ▼, and stable trends with —. These trends are again further qualified as being either positive (■) or negative (■) in character, based on their assessed impact on international stability and security.

The Netherlands in the world (chapter 5). In order to define the position that the Netherlands currently occupies on the world stage, this report provides an overview of Dutch bilateral relations based on four classic dimensions – economic, military, diplomatic, and ideological – and measures the degree of cooperation in those dimensions based on their associated indicators, such as trade volume, arms trade, state visits, and shared values, using the Dutch Foreign Relations Index (DFRI) developed by HCSS.

An assessment of global security perceptions (chapter 6). To gain a better understanding of the security perceptions of other actors, this report looks at over three dozen post-2016 national security and defense strategies published by other countries and survey-based threat analyses published by world-renowned think tanks and intergovernmental organizations. It examines their perceptions of the six threat themes as well as the international order and surveys which other salient threats and opportunities are identified in these documents.

Chapter 7 offers conclusions based on a synthesis of the findings of the chapters listed above.

2 Development of the Threat

This chapter highlights the most important developments that may threaten our national security in the upcoming years. In this chapter, ‘our’ security refers first and foremost to the security of the Netherlands. Of course, Dutch security interests cannot be seen in isolation from the security interests of Europe, the West, and the international community. This wider context is further elaborated on in chapters 3 and 4. As explained in the introduction, the threat themes discussed in this chapter are the six that were identified as the most urgent in the policy white paper *Worldwide for a safe Netherlands: Integrated Foreign and Security Strategy 2018-2022*: military threats, cyber threats, unwanted foreign interference and undermining, threats to vital economic processes, the threat of chemical, biological, radiological and nuclear (CBRN) weapons, and terrorist attacks.²⁴

2.1 Military Competition

Over the past decade, states have been more actively engaging in military competition. States’ perceptions of the security environment have worsened at a time when military threats are becoming more common in the exchanges between rival states. Global military expenditures have increased only marginally, but some major powers have sharply boosted their defense budgets. States are also reprioritizing the modernization of their armed forces, with considerable funds being allocated to emerging technologies such as artificial intelligence (AI) and new operational domains such as space.²⁵ While traditional interstate war remains low in prevalence, the uptick in the number of internationalized intrastate conflicts speaks to increased military competition between states. These findings are corroborated by an analysis of the intentions, capacities, and activities of key states over the past decade (see Table 2), and are further elaborated on below.

24 Separate studies are available on the two online platforms of Clingendael and HCSS: <https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/> and <https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/>.

25 “Foreign Ministers Take Decisions to Adapt NATO, Recognize Space as an Operational Domain, 20-Nov.-2019,” NATO, November 2019.

Table 2 Military competition, multi-factor threat estimate (up to 2025)

Trends	Indicator	
Intentions	Perceptions of Military Competitions in Defense Strategy Documents	▲
	Military Threats	▲
Capability	Military Spending	▲
	Defense R&D and Procurement	▲
Activity*	Interstate Wars	▬
	Violent Crises	▬
	Internationalized Intrastate Conflicts	▲

■ Decreasing threat ■ Increasing threat
▲ Upward ▼ Downward ▬ Net-zero / Stable

2.1.1 Intentions

2.1.1.1 Perceptions of military competition

Military competition is increasingly perceived as an important security priority by major military powers. An analysis of the security and defense strategy documents published by the UK, Germany, France, the US, China, and Russia over the last decade shows a shift toward the identification of interstate competition as a concrete security threat. Both the UK and Germany prioritize interstate competition as a vital security challenge, citing respectively the “resurgence of state-based threats”²⁶ and Europe’s disadvantage in light of increasing international military competition due to its traditionally limited defense budgets.²⁷ France recognizes that “the international balance of power is changing rapidly,”²⁸ stirring greater uncertainty and anxiety. Russia already observed in

26 “National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom” (Her Majesty’s Government, November 2015); “National Security Strategy and Strategic Defence and Security Review 2015: First Annual Report 2016” (Her Majesty’s Government, December 2016).

27 “White Paper 2016: On German Security Policy and the Future of the Bundeswehr” (Federal Ministry of Defense, Germany, June 2016).

28 Republic of France, “Defence and National Security: Strategic Review 2017,” 2017.

2014 that the international order “is characterized by increasing global competition.”²⁹ The US identifies the “re-emergence of long-term strategic competition” and states its aim of consolidating its military edge vis-à-vis rival powers, most notably China and Russia.³⁰ China’s 2019 defense strategy, meanwhile, notes that the “international security system and order are undermined by growing hegemonic behavior, power politics, unilateralism, and constant regional conflicts and wars.”³¹

2.1.1.2 Military threats

The intensification of military competition is apparent not only from state perceptions, but also from the use of threatening rhetoric in exchanges between rival states, especially in the context of a number of long-standing disputes. Using data from the Integrated Crisis Early Warning System (ICEWS), our analysis shows that political and military leaders of permanent members of the UN Security Council have frequently resorted to the use of threatening rhetoric over the past decade with occasional peaks.³² The highest peak was associated with Russia’s annexation of Crimea. Lower peaks in the period since then can be attributed to the US’ placing of sanctions on North Korea,³³ Iran,³⁴ and Russia,³⁵ as well as to the rise in tensions in the South China Sea, and to the Kremlin’s increased engagement in Middle Eastern power politics.³⁶

29 Vladimir Putin, “The Military Doctrine of the Russian Federation,” *Military Doctrine*, December 25, 2014.

30 President of the United States of America, “National Security Strategy of the United States of America” (The White House, 2017).

31 “China’s National Defense in the New Era” (The State Council Information Office of the People’s Republic of China, 2019).

32 ICEWS comprises data from millions of full-text newspaper articles, and applies various coding and natural language processing algorithms to them to extract a series of variables (type of event, actors, geographical location, tone, etc.) on an event-by-event basis. The authors acknowledge issues with using the ICEWS dataset, and events-based datasets in general, including duplication and geographical identification, but submit that - within the context of this study - the large-N query which is made possible by such sources’ incorporation (which cannot feasibly be replicated through other venues) adds tangible value to the research design as a whole, and is fit for purpose when describing larger systemic trends. To correct for changes in the number of articles published over time, the number of filtered events is divided by the number of verbal events on a year-by-year basis.

33 Julian Borger, “Trump Issues New Sanctions on North Korea and Claims China Is Following,” *The Guardian*, September 21, 2017.

34 Eric Walsh and Dave Alexander, “U.S. Slaps Sanctions on Iran Firms after Satellite Launch,” *Reuters*, July 28, 2017.

35 “Russia Expels 755 US Diplomats in Response to Sanctions,” *Al Jazeera*, July 30, 2017.

36 “Turkey’s Downing of Russian Warplane - What We Know,” *BBC News*, December 1, 2015, sec. Middle East.

2.1.2 Capabilities

2.1.2.1 Military spending

Overall levels of absolute military expenditures are increasing internationally, albeit not significantly, and not when measured as a percentage of gross domestic product (GDP). Over the ten-year period from 2008 to 2018, expenditures increased by 13.2%, now amounting to \$1.78 trillion in total.³⁷ The only regions with a significant increase over the past decade are East Asia, Oceania, and the Middle East.³⁸ At the same time, military expenditures saw a decrease in various other regions. Since around 2015, Europe and the US have started to slightly increase their expenditures again, but in other regions, for instance in Latin America, the downward pattern continues or expenditures remain at a low level (relative to the overall level of military expenditures, which are still by far the highest in North America).

Despite substantial regional variation, military expenditures of key military actors have increased considerably. The most striking example is China, which has doubled its military spending from \$120 to \$240 billion in the examined period.³⁹ While official numbers seem to reveal significant recent decreases in Russia's military spending since 2017 (down by 20% to \$66.3 billion), expert reports indicate that a large proportion of real military expenditures are concealed in the state's budget and, when examined closely, could actually turn out to be as much as 40% higher than before.⁴⁰

2.1.2.2 Defense R&D and procurement

After stagnating between 2012 and 2014, military research and development (R&D) budgets are increasing once again. This is largely due to states' pursuit of cutting-edge technologies. This is evident in increases in featured states' R&D budgets, which can be attributed to efforts in military modernization of their armed forces and military capabilities,⁴¹ but also in more specific technology-related investments. Modern technologies' contribution to increases in military R&D are also evident in the uptick in the number of military assets being launched into space, because of

37 "SIPRI Military Expenditure Database (1949–2018)," SIPRI, accessed September 12, 2019.

38 "Trends in World Military Expenditure, 2018," April 2019. The data on the Middle East, which has been an active conflict hotspot for many years now, are inconclusive because of data unavailability for Syria, Qatar, the United Arab Emirates and Yemen, all of which are currently embroiled in conflicts and therefore likely to be increasing their expenditures.

39 "SIPRI Military Expenditure Database (1949–2018)" (SIPRI, September 21, 2019).

40 Vladimir Jushkin, "What Is Hidden in Russia's Military Budget," ICDS, accessed December 9, 2019.

41 Tim Sweijs and Floris Holstege, "Threats, Arms and Conflicts: Taking Stock of Interstate Military Competition in Today's World," Strategic Monitor 2018–2019 (The Hague, Netherlands: The Hague Centre for Strategic Studies, 2019).

states' increasing dependence on space assets in the waging of (interstate) wars.⁴² This ongoing development is illustrative of a wider trend:⁴³ as military competition heats up, new domains and frontiers are commanding strategists' attention.

The US is at the forefront of this trend of increased military R&D spending, focusing on the renewal and modernization of its conventional and nuclear capabilities.⁴⁴ R&D funding for the development of modern technologies received the second-largest percentage increase in the US military budget request for 2019, which was 11% higher than its 2018 precursor.⁴⁵ Other NATO members are increasingly following suit. Recognition of shortcomings in their military R&D efforts resulted in a 50% increase in allocation.⁴⁶ In 2019, NATO members allocated on average 21.7% of their military budget to equipment procurement and R&D, an increase of 1.9% over the preceding year. In 2017, the EU launched the European Defence Fund (EDF), which will make €13 billion available between 2021 and 2027 with the goal of supplementing and amplifying national investments in defense R&D.⁴⁷ The trend is also reflected in China's and Russia's R&D expenditures, with both states implementing a range of programs to modernize their militaries and upgrade their nuclear capabilities.⁴⁸ Russia has committed \$700 billion to an armament program that aims to modernize 70% of Russia's armed forces by 2020,⁴⁹ with 59% of Russia's weapon systems having already been modernized by 2015.⁵⁰

42 Linda Dawson, *War in Space: The Science and Technology Behind Our Next Theater of Conflict* (Springer, 2019).

43 Tim Fernholz, "Jeff Bezos Says Space Isn't a Race. We're Not so Sure," Quartz, accessed December 9, 2019; Joseph Trevithick, "Russia Plans To Launch Tiny Space Plane Off Back Of High Flying M-55 Research Jet," The Drive, accessed December 9, 2019; Namrata Goswami, "The Moon's Far Side and China's Space Strategy," accessed December 9, 2019.

44 See Chuck Hegel, "Reagan National Defense Forum Keynote" (2014); "Nuclear Posture Review 2018" (U.S. Department of Defense, 2018).

45 Susanna V. Blume and Lauren Fish, "Overview of the 2019 President's Budget Request for Defense" (Center for a New American Security (CNAS), February 15, 2018).

46 Michael Shurkin, "The Abilities of the British, French, and German Armies to Generate and Sustain Armored Brigades in the Baltics," Research Report (RAND Corporation, 2017).

47 "EU Budget for the Future," Text, European Commission, 2018.

48 See Anthony Cordesman, *Chinese Strategy and Military Modernization in 2016: A Comparative Analysis* (Washington D.C., USA: Center for Strategic & International Studies, 2016); Julian Cooper, "The Funding of Nuclear Weapons in the Russian Federation" (Changing Character of War Centre, Pembroke College, University of Oxford, October 2018); Cordesman, *Chinese Strategy and Military Modernization in 2016: A Comparative Analysis*.

49 Richard Connolly and Mathieu Boulègue, "Russia's New State Armament Programme" (Chatham House, May 2018).

50 Julian Cooper, "Russia's State Armament Programme to 2020: A Quantitative Assessment of Implementation 2011-2015," 2016.

Beijing has announced intentions to fully modernize its armed forces by 2035,⁵¹ and is focusing on the development of AI applications for military use.⁵² In order to do so, China increased defense spending by 7.5% in 2019, \$177,544 billion of which will be allocated to “sustaining, growing, and modernizing” the country’s military.⁵³

In this context, the size of investments made by the US and China underscores the role of AI applications in modern-day military competition. European states lag behind these countries in their pursuit of military AI,⁵⁴ despite initiatives of individual member states. France, for instance, recently launched a military AI strategy, earmarking €100 million for the development of military AI by 2022.⁵⁵

2.1.3 Activity

Internationalized intrastate conflicts, such as those currently being fought in Libya, Syria, and Yemen, are particular instances of military competition in which states compete for influence in third states’ territories. This type of conflict has increased substantially: it tripled between 2008 and 2018, increasing from six to eighteen. By 2018, such conflicts accounted for 35% of all conflicts (as opposed to 18% in 2008).⁵⁶ This trend stands in contrast to the number of state-on-state military conflicts (interstate war), which comes close to zero, and the number of internal (domestic, civil) conflicts, which stays relatively constant.

Unsurprisingly, the Middle East emerges as a hotspot when it comes to internationalized intrastate conflicts, largely as a result of geopolitical opportunities for foreign meddling brought about by the internal conflicts and power vacuums produced as a by-product of the Arab Spring.⁵⁷ Furthermore, several states are increasing their military footprint

51 Minni Chan, “What’s Driving China’s Military Modernisation Push?,” *South China Morning Post*, August 1, 2017.

52 Elsa Kania, “China May Soon Surpass America on the Artificial Intelligence Battlefield,” *The National Interest* (blog), February 21, 2017.

53 Ankit Panda, “From Hardware to Software: China’s 2019 Military Budget and Priorities,” *The Diplomat*, March 17, 2019.

54 This can be attributed largely to its members’ diverging stances toward autonomous systems or the implementation of the Commission’s AI strategy. Hugo Van Manen, Amit Arkhipov-Goyal, and Tim Sweijs, “Macro Implications of Micro Transformations: An Assessment of AI’s Impact on Contemporary Geopolitics,” *HCSS Security* (The Hague, Netherlands: The Hague Centre for Strategic Studies, August 20, 2019).

55 “Intelligent Design: Inside France’s €1.5bn AI Strategy - Global Defence Technology | Yearbook 2018,” *Global Defence Technology*, 2019.

56 “UCDP - Uppsala Conflict Data Program,” *UCDP - Uppsala Conflict Data Program*, accessed September 12, 2019.

57 “Syrian Civil War Fast Facts,” *CNN*, October 2019.

on the African continent, in the context of wider competition for influence. Chinese and to a lesser extent Russian efforts in this region have attracted a lot of media attention.⁵⁸ The US is also active, for example through the creation of a new drone base in Niger worth \$110 million and the opening of lines of communication with large swathes of North and West Africa.⁵⁹ Power competition over the continent is supplemented by assertive actions of middle powers. Among others, the United Arab Emirates and the Kingdom of Saudi Arabia have set up a peace deal between Ethiopia and Eritrea while securing the rights to military bases, ports, and trading outposts in those countries in the process.⁶⁰ These developments do not neatly fall into the ‘activity’ category of military competition, in that they represent other forms of engagement, but they are nonetheless indicative of increasing awareness of the continent’s strategic importance, both militarily and otherwise.

As geopolitical rivalry is regaining prominence, the threat posed to the Netherlands by military competition has increased significantly – not so much in a direct threat to our territorial integrity, but certainly in an increased risk that the Dutch armed forces, together with the country’s allies, will find themselves embroiled in a future military confrontation.

2.2 Cyber Security

Conflict in cyberspace has intensified exponentially in recent years.⁶¹ Our analysis of the intentions, capabilities, and activities of state actors in this domain suggests that this is unlikely to change in the near future, with greater risks of escalation. Cyber-military and cyber-security expenditures have increased, as have cyber-enabled espionage and computer network attacks. Disinformation campaigns are the new normal in global affairs. States regard threats emanating from cyberspace as a crucial security concern.

58 Abdi Latif Dahir, “Russia Is the Latest World Power Eyeing the Horn of Africa,” *Quartz Africa*, March 9, 2018; Michael Kovrig, “China Expands Its Peace and Security Footprint in Africa,” *Crisis Group* (blog), October 24, 2018.

59 Johannes Thimm, “From Exception to Normalcy,” SWP - Stiftung Wissenschaft und Politik/German Institute for International and Security Affairs, October 2018.

60 “The United Arab Emirates in the Horn of Africa,” Middle East Briefing N65 (Abu Dhabi: International Crisis Group, November 6, 2018).

61 The analysis of activities in cyberspace also includes actions that are not directly linked to states. For example, the analysis of Computer Network Attacks is based on reported instances against a government agency, but the data also includes attacks against defense companies and high-tech companies, as well as economic crimes with a loss of more than \$1 million. Therefore, although not every data point corresponds directly to a state actor, these events still have an economic and/or security impact on states.

Table 3 Cyber Security, multi-factor threat estimate (up to 2025)

Trends		Trend
Intention	States disclosing offensive cyber capability to enhance transparency	▲
	Perceptions of interstate escalation of tensions in cyberspace	▲
Capacity	Cyber military spending	▲
	National cybersecurity & counter cybercrime spending	▲
Activity	Reported Cyber Enabled Espionage (CNE)	▲
	Reported Cyber Enabled Attacks (CNA)	▲
	Disinformation campaigns	▬

■ Decreasing threat ■ Increasing threat
▲ Increase ▼ Decrease ▬ Net-zero / Stable

2.2.1 Perceptions of interstate escalation of tensions in cyberspace

An increasing number of states identify cybersecurity as either the main or a major security threat in their national security threat assessments.⁶² Previous strategies (2006-2013) already acknowledged the relevance of various cyber threats, such as cybercrime, IP theft, espionage, and sabotage. Recent strategies (2015-2019) more specifically single out the threat posed by state actors and state-affiliated or directed cyber operations for offensive purposes, underscoring the relevance of cyberspace for national security. In this context, states have been developing initiatives to address risk management of cyber escalation.⁶³ Most notably, the application of international law, norms of

62 Throughout all eight analyzed National Security Strategies (US, DE, FR, UK, CN, RF, IN, NL). See for example Daniel Coats, “Worldwide Threat Assessment of the US Intelligence Community” (Senate Select Committee on Intelligence, January 29, 2019). This risk is echoed in the recent Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (7823/2/17 REV 2): “The EU is concerned about the increased ability and willingness of state and non-state actors to pursue their objectives by undertaking malicious cyber activities of varying in scope, scale, duration, intensity, complexity, sophistication and impact.”

63 For more information initiatives see the “International Order in Cyberspace” section below.

responsible state behavior, and confidence-building measures (CBMs) have functioned as stability mechanisms that establish ‘rules of the road’ for responsible state behavior in cyberspace. Over the last couple of years, the cyber-strategic postures of leading states have evolved to include the more offensive deterrence by punishment, complementing deterrence by denial, entanglement, and normative stigmatization. This is illustrated, for example, by the US doctrine of “persistent engagement” that is designed not only to thwart adversary cyber operations by continuously anticipating and exploiting their vulnerabilities, but also to reinforce deterrence by raising the costs for adversaries.⁶⁴

2.2.2 States disclosing offensive cyber capabilities to enhance transparency

The lack of transparency in cyber capability deployment, and even in the method of operations or intended effects, renders the task of assessing a state’s intentions, capabilities, and activities difficult.⁶⁵ Based on an open-source analysis of public statements, we observe a growing number of states disclosing their offensive cyber capabilities. The US National Security Agency puts the current number at thirty.⁶⁶ It signifies the progressive militarization of cyberspace. To some degree, it also points toward efforts at increasing transparency, which is necessary for the development of rules and norms to harness competition in this domain.

2.2.3 Assessing spending on cyber capabilities

Government funding to enhance cybersecurity can be perceived as either heightening or reducing the threat level in this environment, depending on whether the spending is directed toward defensive or offensive measures. We therefore distinguish between ‘national cybersecurity and counter cybercrime spending’, which is defensive by nature, and ‘cyber-military spending’, which includes both offensive and defensive capabilities. A review of open-source documents and budgets of eight Western countries shows

64 United States of America Department of Defense, “Cyber Strategy” (U.S. DoD, 2018); President of the United States of America, “National Security Strategy of the United States of America.”

65 Alexander Klimburg and Louk Faesen, “A Balance of Power in Cyberspace | HCSS,” *European Cybersecurity Journal* 3, no. 4 (2018).

66 James R. Clapper, Marcel Lettre, and Michael S. Rogers, “Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States” (U.S. Senate Armed Services Committee, January 5, 2017).

current government spending has increased in both categories.⁶⁷ The US remains at the forefront of cybersecurity spending, with countries such as France and the UK following suit. The rise in investment in defensive measures is also indicated by the creation of dedicated agencies and departments that focus on cybersecurity. As a reflection of the increase in states disclosing offensive cyber capabilities, cyber-military spending is also rising. The US leads this trend, with significant portions of the 2019 annual budget being allocated to the US Cyber Command.⁶⁸ Under both the Obama and Trump administrations, the capabilities of the US SCyber Command have expanded through an increase in personnel, a greater operational mandate, and enhanced technical capabilities.⁶⁹ Although overall military spending on cybersecurity is significantly lower in the other examined countries, their investments in offensive cyber capabilities have also grown.

2.2.4 Cyberespionage

In cyberspace, states may hide under a veil of anonymity to engage in malign cyber activity, in order to achieve strategic and operational gains. States have been more aggressively engaging in various activities: computer network exploitation, which includes cyberespionage; computer network attacks, which include attacking the availability and integrity of data and ICT systems; and disinformation campaigns. While attribution remains complicated, targeted states are increasingly naming and shaming malign actors.⁷⁰ The past ten years saw a considerable rise in reported instances of cyberespionage, according to data from the Cyber Operations Tracker of the Council on Foreign Relations.⁷¹ China in particular is reported to be engaging in intellectual property

67 This report used only publicly available sources and data, preventing it from giving absolute numbers and findings. Determining cybersecurity spending is challenging because: (i) of the lack of consistent reporting; (ii) the absence of a unified definitions, which makes it difficult to delineate which costs are specifically attributed to cybersecurity per se; (iii) cybersecurity is increasingly evolving into the integral part of government operations – rather than being a separate cost unit; (iv) collecting and mapping the data of ICT and cybersecurity investments is generally complicated as cybersecurity is mostly approached qualitatively, and not primarily from a cost perspective.

68 “The agency is executing on a fiscal year budget of about \$610 million in 2019,” Lauren C. Williams, Lauren Williams, “Cyber Command Looks to Expand,” FCW, February 2019.

69 Jim Garamone and Lisa Ferdinando, “DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command,” *U.S. Department of Defense*, August 18, 2017.

70 See for example Foreign & Commonwealth Office and National Cyber Security Centre, “Press Release: UK Exposes Russian Cyber Attacks,” GOV.UK, October 4, 2018.

71 Due to the clandestine nature of cyber espionage, this data is limited in the degree to which it adequately captures all cyber espionage as it occurs. This data reflects reported cyber espionage, but as actors are increasingly sophisticated in their activities, cyber espionage often remains undetected.

and advanced military technology theft through its PLA Unit 61398 as well as other government units.⁷²

2.2.5 Computer Network Attacks

Similarly, Computer Network Attacks are increasingly prevalent. According to the Center for Strategic and International Studies, the number of reported significant cyber incidents increased seven-fold between 2008 and 2018.⁷³ Denial of service, domain name system (DNS) hijacking campaigns, malware attacks, phishing, and ransomware attacks seek to damage, destroy, or disrupt computers and/or computer operations,⁷⁴ with direct or indirect negative impacts on states.⁷⁵ Notable Computer Network Attacks include: Stuxnet (2010); the attack on Saudi Arabia's oil infrastructure in 2012; attacks against the Ukrainian power grid (2015); North Korea's targeting of Microsoft Windows computers (WannaCry, 2017); and Russia's release of NotPetya (2017).⁷⁶

72 Geoffrey Ingersoll, "China Hacking: P.L.A. Unit 61398," *Business Insider*, 61398, accessed November 7, 2019; David E. Sanger and Steven Lee Myers, "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology," *The New York Times*, November 29, 2018, sec. U.S.

73 The Center for Strategic and International Studies (CSIS) has logged "significant cyber attacks" since 2006. Events are included in this list on the basis of whether the attack was against a government agency, defense company, or high-tech company, or was an economic crime with a loss of more than \$1 million. Events were coded and categorized by HCSS, and then included in the analysis depending on the type of incident. "Significant Cyber Incidents," Center for Strategic and International Studies, accessed December 9, 2019.

74 Kim Zetter, "Hacker Lexicon: What Are CNE and CNA?," *WIRED*, June 7, 2016.

75 The analysis of Computer Network Attacks (Table 2) is based on reported instances of CNA against a government agency, but the data also includes attacks against defense companies and high-tech companies, as well as economic crimes with a loss of more than a million US dollars. Therefore, although not every data point corresponds directly to a state actor, these events still have an economic and/or security impact on states.

76 See Appendix B of the cyber report, on the strategic monitor website: 'Timeline of Major Cyber Incidents 2007-2019'. See also "Significant Cyber Incidents." Notable examples include the attack on Iran's nuclear program (Stuxnet, 2010) (see Richard Spencer, "Stuxnet Virus Attack on Iranian Nuclear Programme: The First Strike by Computer? - Telegraph," *The Telegraph*, October 2010), the attack on Saudi Arabia's oil infrastructure in 2013 (see Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival* 55, no. 2 (April 2013): 81–96.), Russia's attack on the Ukrainian power grid (2015) (Elias Groll, "Did Russia Knock Out Ukraine's Power Grid? - Foreign Policy," *Foreign Policy*, January 2016), Russia's hacking of the DNC in the US (2016) (see Spencer Ackerman, "US Officially Accuses Russia of Hacking DNC and Interfering with Election," *The Guardian*, accessed November 7, 2019), the DPRK's targeting of Microsoft Windows computers (WannaCry, 2017) (see Dustin Volz, "U.S. Blames North Korea for 'WannaCry' Cyber Attack," *Reuters*, December 2017) and Russia's release of NotPetya (global, 2017) (see Sarah March, "US Joins UK in Blaming Russia for NotPetya Cyber-Attack," *The Guardian*, February 2015).

2.2.6 Disinformation campaigns

Cyber-enabled disinformation campaigns are increasing too. Although there is no comprehensive data source providing reliable data for the past decade, an abundance of studies and reports highlight how states are engaging in comprehensive disinformation campaigns to influence public perception and erode trust in democratic systems.⁷⁷ According to the Oxford Internet Institute, the number of states featuring active disinformation campaigns more than doubled from 28 to 70 between 2017 and 2019. At least seven states (China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela) have executed influencing campaigns in other countries.⁷⁸ Recent technological developments in this field – including the rise of ‘deep fakes’, i.e., hyper-realistic, difficult-to-debunk fake videos – are expected to further affect the nature and impact of disinformation campaigns.⁷⁹ At the same time, efforts to counter disinformation campaigns are increasing, especially in European countries.⁸⁰ Overall, our analysis of perceptions, intentions, capabilities, and activities of states in the cyber domain warrants the conclusion that cyber conflict is intensifying, and is likely to continue to do so in the years to come.

2.3 Hybrid Conflict

Hybrid conflict, understood as “conflict between states, largely below the legal level of armed conflict, with integrated use of civilian and military means and actors, with the aim of achieving certain strategic objectives,”⁸¹ has become much more prominent over the past decade. States are increasingly deploying hybrid tactics, often in a subtle and pervasive form to hamper detection, accountability, and retaliation. These tactics include the use of proxy actors in third-party military conflicts, the deployment of military exercises near borders, intrusions into aerial and maritime territory, the exertion of influence over foreign democratic processes, the use of economic coercion, the proliferation of disinformation campaigns, and the execution of cyberattacks on critical

77 Kanzanira Thorington, “Europe’s Elections: The Fight Against Disinformation,” *Council on Foreign Relations* (blog), May 23, 2019.

78 Samantha Bradshaw and Philip Howard, “The Global Disinformation Order: 2019 Global Inventory Of Organised Social Media Manipulation,” Working Paper (Oxford, United Kingdom: Oxford Internet Institute, 2019).

79 Robert Chesney and Danielle Citron, “Disinformation on Steroids: The Threat of Deep Fakes,” *Cyber Brief* (Council for Foreign Relations, October 16, 2018).

80 Daniel Funke and Daniela Flamini, “A Guide to Anti-Misinformation Actions around the World,” Poynter, 2018.

81 Translation of the Dutch definition taken from “Χίμαιρα: Een Duiding van Het Fenomeen ‘hybride Dreiging” (NCTV, April 2019).

infrastructure. Our analysis of intentions, capabilities, and activities in this sphere paints an overall bleak outlook (see Table 4).⁸²

2.3.1 States' perception of hybrid conflict as a threat to national security

Comparative assessments of security and defense strategies between 2008–2009 and 2018–2019 reveal that states increasingly recognize hybrid conflict as a threat to national security.⁸³ The US currently identifies cyber conflict, disinformation campaigns, and economic coercion, explicitly designating China, Russia, and Iran as culprits.⁸⁴ Germany and the Netherlands are particularly concerned about cyber threats and information warfare. Germany moved from signaling a “digital lack of security”, but without mentioning “hybrid”, in 2008 to explicitly identifying hybrid conflicts as a security risk in 2018.⁸⁵ The Dutch Integrated International Security Strategy (2018) illustrates hybrid conflict with threats such as foreign interference through disinformation, cyberespionage, sabotage, and foreign funding.⁸⁶ Over a ten-year period, the UK exhibits a heightened awareness of hybrid threats in the cyber and political domain.⁸⁷ But the recognition of hybrid threats is not exclusive to Western countries. Russia points out risks posed by external manipulation and subversion, noting that “[t]he intensifying confrontation in the global information arena caused by some countries’ aspiration to utilize informational and communication technologies to achieve their geopolitical

82 The states looked at for the *Perception, Intention, Capability*, and *Activity* trend assessments were selected based on their relevance to the Dutch threat environment, the availability of open-source defense strategies and the objective to cover a range of different actors. The resulting set comprises the Netherlands (in order to gauge the perceptions and capabilities of the referent state), the close allies France, Germany, the UK, and the US, and the two major powers China and Russia. The various *Activities* trends were conducted with a broader scope, although many examples again pertain to the state actors mentioned.

83 Where possible, the years 2009–2019 were analyzed. However, due to incomplete data from 2019 (given that the Global Security Pulse was published in October) it was mostly more fitting and accurate to analyze the years 2008–2018.

84 Daniel Coats, “Worldwide Threat Assessment of the US Intelligence Community,” 5; Dennis Blair, “Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence” (Director of National Intelligence, February 2009).

85 “Weißbuch 2006 Zur Sicherheitspolitik Deutschlands Und Zur Zukunft Der Bundeswehr” (Bundesministerium der Verteidigung, October 2006); “Weissbuch 2016: Zur Sicherheitspolitik Und Zur Zukunft Der Bundeswehr” (Die Bundesregierung, July 2016); Ministry of Foreign Affairs, “Working Worldwide for the Security of the Netherlands: An Integrated International Security Strategy 2018–2022” (Ministry of Foreign Affairs, March 20, 2018); “Strategy and Work Programme 2007–2008” (ECFR, May 2007), 2007–8.

86 Ministry of Foreign Affairs, “National Security Strategy 2018.”

87 “National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom,” 19; “The National Security Strategy of the United Kingdom: Update 2009” (Cabinet Office, June 2009).

Table 4 Hybrid conflict, multi-factor threat estimate (up to 2025)

Trends		
Perception	States' perception of hybrid conflict as a threat to their national security	▲
	States' intention to use hybrid means as part of their defence strategies	▲
Capability	Capacity of states to engage in and/or respond to hybrid conflict	▲
Military Activity	The use of proxies by state actors in third party military conflicts	▲
	Military exercises near borders	▲
	Aerial and maritime intrusions	▲
Political Activity	External meddling in domestic politics	▲
Economic Activity	Economic coercion	▲
Information Activity	Disinformation campaigns	▲
Civil Activity	Cyberattacks on critical infrastructure	▲

■ Decreasing threat ■ Increasing threat
▲ Upward ▼ Downward ■ Net-zero / Stable

objectives, including by manipulating public awareness and falsifying history, is exerting an increasing influence on the nature of the international situation.⁸⁸ China, too, makes reference to hybrid threats emanating from the US, through the use of sanctions and political provocation.⁸⁹ In contrast to its 2008 equivalent, China's 2019 defense white paper mentions hybrid threats, including the rise of cyber-related threats, the potential use of sanctions against companies and academics, and other states' financial support of Tibet's freedom movement.⁹⁰

2.3.2 States' intention to use hybrid strategies

Having pioneered strategic innovation in this sphere over the past decade, Russia emphasizes "cross-domain coercion" as part of its strategic deterrence posture, which combines both military (conventional and nuclear) and non-military capabilities and measures.⁹¹ China's latest defense strategy reserves "the option of taking all necessary measures" to safeguard China's national sovereignty, security, and interests.⁹² Overall, such intentions are expressed to a greater extent than ten years ago,⁹³ although Western states thus far have predominantly framed this within a defensive context of countering hybrid activities. The cyber domain represents an exception to this tendency, as states increasingly disclose their intentions to use offensive cyber measures against other states.⁹⁴ The UK, for instance, stresses its willingness to use armed force to defend itself from cyberattacks and to protect its networks, if attacking the networks of the attacker is necessary.⁹⁵

2.3.3 States' capabilities to engage in and/or respond to hybrid conflict

States are increasingly investing in government agencies that engage in or respond to hybrid conflict. China, Russia, the US, France, Germany, the UK and the Netherlands have all created, invested in and widened the scope of such government agencies over the past ten years. In addition to employing public organizations and agencies, many

88 "Russian National Security Strategy," December 2015.

89 "China's National Defense in the New Era."

90 "China's National Defense in the New Era."

91 "Russia: National Security Strategy to 2020," *ETHZ* (blog), May 2009; "Russian National Security Strategy."

92 "China's National Defense in the New Era," 7.

93 Daniel Coats, "Worldwide Threat Assessment of the US Intelligence Community," 5.

94 See Appendix A in Louk Faesen et al., "Conflict in Cyberspace: Parsing the Threats and the State of International Order in Cyberspace" (HCSS, November 2019).

95 "National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom."

states carry out hybrid operations through non-state actors or covert units.⁹⁶ Russia's capabilities are illustrated by the increased role of the Russian Main Directorate of the General Staff of the Armed Forces (commonly referred to as the GRU), as well as the Russian Internet Research Agency, which is involved in "bot farms" and disinformation campaigns.⁹⁷ In China, the People's Liberation Army (PLA) Strategic Support Force (home to Unit 61398, among others) has been mentioned by experts as a hybrid-focused force, with tasks including information warfare and cyber operations. China's whole-of-government approach to conflict and security means that several government agencies, not specifically designated as 'hybrid' actors, may play a coordinated role in these activities.⁹⁸ The US Cyber Command is another example of a military-focused agency with an important role in hybrid conflict, as exemplified by a cyberattack the Command undertook in Iran during July 2019.⁹⁹ In Europe, for instance, the Netherlands has established a Counter Hybrid Unit.

2.3.4 The use of proxies by state actors in third-party military conflicts

Just as in the Cold War, states are engaging in proxy conflicts.¹⁰⁰ Proxy conflicts arise when states "instigate or play a major role in supporting and directing a party to a conflict," but do only a small portion of the fighting themselves.¹⁰¹ These conflicts allow states to secure ideological and/or strategic objectives without putting a significant number of their own troops in harm's way. Proxy wars also offer the opportunity to test and showcase new weapon systems, facilitating a learning process that would

96 "Chinese Public Diplomacy in Taiwan" (NATO Strategic Communications Center of Excellence, June 2019); Bettina Renz, "Russia and 'Hybrid Warfare,'" *Contemporary Politics* 22, no. 3 (July 2, 2016): 283–300.

97 Jean-Baptiste Jeangene Vilmer et al., "Information Manipulation: A Challenge for Our Democracies" (Paris, France: Policy Planning Staff of the Ministry for Europe & Foreign Affairs and the Institute for Strategic Research at the Ministry for the Armed Forces, August 2018); Robert Mueller, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election" (Washington D.C., USA: U.S. Department of Justice, March 2019).

98 Peter Mattis, "China's 'Three Warfares' in Perspective," *War on the Rocks* (blog), January 30, 2018; Adam Ni and Bates Gill, "The People's Liberation Army Strategic Support Force: Update 2019," *China Brief*, May 29, 2019; Kevin Pollpeter, Michael Chase, and Eric Heginbotham, "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations," Research Reports (California, United States of America: RAND Corporation, 2017); Lyle J. Morris et al., "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War," Product Page (RAND Corporation, 2019).

99 Julian E. Barnes, "U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say," *The New York Times*, August 28, 2019, sec. U.S.

100 Mazarr et al., *Understanding the Emerging Era of International Competition*.

101 Daniel L. Byman, "Why Engage in Proxy War? A State's Perspective," *Brookings* (blog), May 21, 2018.

otherwise only be available within the context of interstate conflicts.¹⁰² Proxy wars can be understood as a form of hybrid conflict, not only because they are also a form of gray zone operations – as can be inferred from states’ systematic denial of involvement in these conflicts¹⁰³ – but also because there are well-documented instances of these activities being employed to secure objectives that fall outside these conflicts’ direct geographical scope. In addition to the earlier-reported steep increase in the number of internationalized intrastate conflicts – which with eighteen conflicts account for 35% of all conflicts in 2018 (as opposed to 18% in 2008)¹⁰⁴ – the number of actors involved in these proxy conflicts has increased from an average of 3.7 actors per proxy conflict in 2008 to 5.8 actors in 2018.¹⁰⁵ The upward trend in the use of proxy forces extends into cyberspace, where states increasingly rely on cybercriminals as extensions of state power.¹⁰⁶

2.3.5 Military exercises near borders

Military exercises near the borders of actual or potential adversaries are a well-established practice, meant to intimidate without crossing the threshold into conventional conflict. Without any effective confidence- and security-building measures (CSBMs) in place, these military exercises have the potential to exacerbate instability and lead to escalatory retaliations. Military exercises near borders have increased in number and in magnitude over the last ten years.¹⁰⁷ Especially over the last five years, after the Crimea Crisis, they have become both larger in scale and more regular in occurrence, both in Europe and in Asia.

2.3.6 Aerial and maritime intrusions

Similarly, aerial and maritime activities that stay below the threshold of actual confrontations seem to be increasing. Intrusions are exercises that deliberately and provocatively enter other states’ territories (or threaten to do so). Measurements reveal a slight upward incline in interceptions of Russia’s aerial activities over NATO territory, but also a more striking trend toward indirect interferences that provokingly

102 Dario Leone, “Did Russia’s Deadly Su-57 Stealth Fighter Get Ready for ‘War’ in Syria?,” *The National Interest*, August 31, 2019.

103 Claire Graja, “SOF and the Future of Global Competition” (CNA, May 2019).

104 “UCDP - Uppsala Conflict Data Program.”

105 “UCDP - Uppsala Conflict Data Program.”

106 Alexander Klimburg, “Cybercriminals as Extensions of State Power?” (ISPI, July 2018).

107 Though expert analysis shows that military exercises near borders have increased over the ten-year period, the quantitative data to reflect this increase is difficult to acquire due to the classified nature of the content and sizable disparities between the announced numbers of involved personnel and the actual number of personnel.

threaten, but do not violate, NATO territory. Similarly, expert analyses reveal that, since 2008, Chinese military naval activities have increased in the East and South China Sea.¹⁰⁸ According to the Japanese Foreign Ministry, the number of vessels within Japan's territorial waters and the contiguous zone rose in 2012 and has since remained consistently high.¹⁰⁹ The number of vessels in the contiguous zone is approximately twice as high as that witnessed in territorial waters, speaking to the notion that most Chinese maritime activities have not directly violated littoral states' territorial integrity, but have rather taken a more blurred approach, typical of the hybrid domain. In 2017, this number spiked considerably, which can be linked to a more aggressive approach taken by China in the first half of 2017 when it departed from sending only ships into the disputed territories and began also to use unmanned aircraft.¹¹⁰ Overall, the Chinese are increasingly employing both military and paramilitary law enforcement ships in order to patrol and curb the influence of other actors in the waters.¹¹¹

2.3.7 Political activity

Exploiting the networked nature of information societies, political interference has surged. Meddling activities include, but are not limited to, disinformation campaigns, cyberattacks, and economic coercion. As reported in chapter 2.2, disinformation campaigns have greater reach and impact than ever before.¹¹² In addition to well-reported cases, such as the 2016 US election interference, political meddling as a hybrid tactic occurs on a global scale.¹¹³ In Western Europe, cyberattacks and disinformation campaigns are more common than elsewhere,¹¹⁴ whereas countries in the Western

108 Tetsuo Katani, "China and Russia in the Western Pacific: Implications for Japan and the United States," *The National Bureau of Asian Research (NBR)* (blog), accessed December 9, 2019; "Military and Security Developments Involving the People's Republic of China 2019" (US. Dept. of Defense, May 2, 2019).

109 "Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan's Response," Ministry of Foreign Affairs of Japan, accessed December 9, 2019.

110 Yoko Wakatsuki and Junko Ogura, "Japan: China 'escalating' Tensions over Disputed Islands," CNN, accessed December 9, 2019.

111 NBR *ibid.*; Office of the Secretary of Defense *ibid.*

112 Bradshaw and Howard, "The Global Disinformation Order: 2019 Global Inventory Of Organised Social Media Manipulation"; Britt Paris and Joan Donovan, "Deepfakes and Cheap Fakes" (United States of America: Data & Society, October 18, 2019).

113 Bruce Jones and Torrey Taussig, "Democracy & Disorder: The Struggle for Influence in the New Geopolitics" (Brookings, February 2018).

114 Danuta Gibas-Krzak, "The Political, Economic and Cultural Influences of Neo-Ottomanism in Post-Yugoslavian Countries. An Analysis Illustrated with Selected Examples," *POLSKA AKADEMIA UMIEJ TNO CI* 26 (2017); Arlinda Rustemi et al., "Geopolitical Influences of External Powers in the Western Balkans" (HCSS Security, September 30, 2019); Paul Stronski and Anne Himes, "Russia's Game in the Balkans," January 2019.

Balkans tend to be victims of economic coercion and corruption.¹¹⁵ Russia's activities include cyberattacks, disinformation campaigns, and economic coercion such as exploiting its energy resources.¹¹⁶ Russia also uses proxy organizations, such as the Wagner Group, to exercise pro-Kremlin influence in Europe, the Middle East, and Africa. China also embarks on information campaigns, as well as engaging in persistent state-sponsored espionage and the fostering of economic dependencies on a global scale, which it can exploit for political purposes.¹¹⁷

2.3.8 Economic activity

States are increasingly resorting to coercive economic measures to achieve their political objectives by exploiting economic vulnerabilities and dependencies.¹¹⁸ An analysis of Global Trade Alerts reveals a massive surge in 'harmful measures' associated with economic coercion between 2008 and 2018. In addition, economically coercive events, as reported in the Integrated Crisis Early Warning System (ICEWS), such as sanctions, boycotts, and embargos, have also increased considerably. This has been clearest in recent years, with the US becoming much more assertive. A spike occurred in 2018, with US measures aimed at China and Chinese state-owned enterprises, Iran and Iranian officials, Russia, and Turkey.¹¹⁹

115 Naja Bentzen, "Foreign Influence Operations in the EU" (Members' Research Service, July 2018); Jeangene Vilmer et al., "Information Manipulation."

116 Jason Bordoff and Trevor Houser, *American Gas to the Rescue? The Impact of US LNG Exports on European Security and Russian Foreign Policy* (New York, United States of America: Columbia University, 2014); *Cyber Attacks Controlled by Intelligence Services* (Bundesamt für Verfassungsschutz, 2018); Adam B. Ellick and Adam Westbrook, "Opinion | Operation Infektion: A Three-Part Video Series on Russian Disinformation," *The New York Times*, November 12, 2018; Anna Reynold, *Redefining Euro-Atlantic Values: Russia's Manipulative Techniques* (Riga, Latvia: NATO Strategic Communications Center of Excellence, 2017); Bentzen, "Foreign Influence Operations in the EU"; Natalie Slobodian, "Political Technologies of Russian Energy Diplomacy," *Nowa Polityka Wschodnia* 16, no. 1 (March 2018): 49–65; Stronski and Himes, "Russia's Game in the Balkans"; Dimitar Bechev, *Understanding Russia's Influence in the Western Balkans* (The European Center of Excellence for Countering Hybrid Threats, 2018); Hongchan Chun, "Russia's Energy Diplomacy toward Europe and Northeast Asia: A Comparative Study," *Asia Europe Journal*, 2009.

117 Bentzen, "Foreign Influence Operations in the EU."

118 A challenge inherent in classifying and measuring economic coercion is that, unlike other types of influencing, this type of coercion can be easily disguised as measures of protectionism. See for example Dong-Hun Kim, "Coercive Assets? Foreign Direct Investment and the Use of Economic Sanctions," *International Interactions* 39, no. 1 (January 1, 2013): 99–117.

119 Based on analysis of CAMEO codes: 1312, 163, 1711 in ICEWS data.

2.3.9 Information activity

As reported in chapter 2.2.6, disinformation campaigns have become much more prevalent, with the explicit intent to manipulate democratic discourses and stir up societal disarray, polarization, and impact on democratic processes. The reach and impact of recent campaigns have increased through strategic and technological innovation.¹²⁰ Disinformation campaigns vary by perpetrator, methodology, and motivation. While Western understanding of modern disinformation is predominantly shaped by Russian activities, an increasing number of states are also active in this domain. India, Iran, North Korea, and Saudi Arabia, amongst others, are developing capabilities in information manipulation.¹²¹ China is also becoming more active in this field.¹²²

2.3.10 Cyber activity

As reported in chapter 2.2, the number of cyberattacks on states' critical infrastructure has also increased sharply over the past ten years. Examples include the 2012 cyberattack on the Saudi national oil company Saudi Aramco and two attacks perpetrated in 2015: the 'WannaCry' ransomware attack on the UK's National Health Service and the attack on Ukraine's energy distribution company. In 2018, the US Government warned that actors associated with the Kremlin were conducting cyber reconnaissance on energy, nuclear, water, and other critical infrastructure sectors in the US, possibly in preparation for targeted attacks. An assessment of the most significant cyber incidents reveals that most attacks on critical infrastructure were state-on-state in nature.¹²³ The most frequent actors to target other states' critical infrastructure were Russia, China, and Iran, closely followed by North Korea. The main targets of such

120 Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0" (Washington D.C., USA: Atlantic Council, June 2019), 0.

121 *Hybrid Threats: A Strategic Communications Perspective* (Riga, Latvia: NATO Centre of Excellence, 2019); Owen Pinnell, "The Online War between Qatar and Saudi Arabia," BBC News, June 3, 2018; *Who Said What?: The Security Challenges of Modern Disinformation* (Canadian Security Intelligence Service, 2018); Paris and Donovan, "Deepfakes and Cheap Fakes."

122 Mattis, "China's 'Three Warfares' in Perspective"; "Chinese Public Diplomacy in Taiwan"; Daniel R. Coats, "Statement for the Record," Worldwide Threat Assessment of the US Intelligence Community (Washington, D.C.: Senate Select Committee on Intelligence, 2019).

123 "Significant Cyber Incidents." n 126 ??

cyberattacks have been the US, South Korea, India, and Ukraine.¹²⁴ Many of the reported events do not take place during a military conflict, but in the gray zone.¹²⁵

Overall, our analysis corroborates the conclusion that hybrid threats have proliferated within the international security environment. States are engaged in a range of hybrid activities and are gearing up for competition in the gray zone. In the military domain, the increased prevalence of hybrid conflict is substantiated by rising trends in the use of proxy actors, the frequency and scale of military exercises near borders, and the number of aerial and maritime intrusions. External meddling in domestic politics has become more widespread. Economic coercion is becoming more common. Hybrid strategies also extend to the information and cyber domains, where the dissemination of false information and cyberattacks on critical infrastructure have increased considerably.

2.4 Economic Security

Geopolitical competition is currently reshaping the global economy, and economic power and instruments are increasingly used for political purposes. Simultaneously, the fast-changing and increasingly complex contemporary geopolitical context has shifted increasing attention to economic security. It is developments like these that illustrate that economics, politics, and geopolitics have become more interwoven. Hence, it is not surprising that economic security has been receiving increased attention from both European and Dutch policymakers. In the field of economic security, the results of our horizon scan give cause for concern. Even though some positive developments can also be witnessed, there are increasing concerns, in particular when it comes to trade tensions and economic espionage. Table 5 provides an overview of the different threat-related trends and developments in the field of economic security.

124 Note the low presence of attacks against China or Russia, which could point to a lack of reporting from these states regarding cyberattacks. This logic may follow an internal power dynamic of not admitting internal weakness in the cyber domain or be reflective of a representation bias (e.g., underrepresenting retaliation attacks by India that have not been reported by Pakistan).

125 “Significant Cyber Incidents”; “Cyber Operations Tracker,” Council on Foreign Relations, accessed December 20, 2019.

Table 5 Economic security, multi-factor threat estimate (up to 2025)

Trends	Indicator	Trend
Trade tensions	Trade protectionism: export and other subsidies, tariff measures, trade-protective measures, government procurement restrictions	▲
	Level of WTO dispute settlement activity	▼
	Economic freedom	▼
Open trade routes	Global seaborne trade (80% of total trade in goods)	▲
	Number of piracy attacks	▼
	Vulnerability of maritime chokepoints	▲
FDI and takeovers	FDI regulatory restrictiveness	▲
Energy and raw materials	Energy dependence of EU (gas, petroleum, solid fuels)	▲
	(Critical) raw materials dependence of EU	▲
Economic espionage	Threat level of economic (cyber) espionage NL/EU	▲

■ Decreasing threat ■ Increasing threat
▲ Upward ▼ Downward — Net-zero / Stable

2.4.1 Open trade routes

Conflicts in countries surrounding the Suez Canal and the influence of Russia and China in the region potentially affect trade routes. For example, unrest in the Horn of Africa could threaten navigation in the southern entrance to the Red Sea, thereby possibly affecting access to Egypt's Suez Canal. Moreover, Egypt has been making diplomatic overtures to Moscow and Beijing, as the US' involvement has diminished. Egypt and China have already signed deals worth \$18 billion as part of the Belt and Road Initiative (BRI). In addition, Egypt recently signed deals with Russia to establish a Russian industrial zone around the Suez Canal. Chinese and Russian influence could potentially endanger access to this important trade corridor.¹²⁶

Another potential threat originates from pirate attacks and armed robberies in West Africa. After a period of decline, the number of pirate attacks and armed robberies has recently been on the rise. West Africa has overtaken the Horn of Africa as Africa's piracy hotspot. According to the International Maritime Bureau's annual report, pirate attacks and armed robberies rose worldwide between 2017 and 2018, with a surge of attacks off West Africa, despite declining numbers in other parts of the world. Petro-piracy in particular is a growing risk off West Africa and can affect oil supplies to the EU.¹²⁷

2.4.2 FDI and takeovers

China has become increasingly active with foreign direct investment in the EU, enhancing its political influence. Greece, Portugal, and Malta have already signed deals with China, in sectors ranging from energy to transportation, in addition to a significant Chinese presence in insurance, health, and financial services. Italy – the first G7 member and the third-largest EU economy – has signed deals worth €2.5 billion. That figure could potentially rise to €20 billion, since the two countries have pledged closer economic cooperation, particularly in the fields of connectivity, (energy) infrastructure, and trade. In its wake, several EU member states signed an agreement within the BRI framework. Even though these investments are relatively small, and projects may fail, the political significance may be great. In other countries, similar investments have led to the emergence of debt traps or divergent voting in international organizations. In the future,

126 Maxamuud Axmed, "Egypt, Somalia Bolster Security Coordination Amid Suez Canal Fears. | Somaliweyn," *Somaliweyn*, March 2019; "Russia Announces Establishing Industrial Zone in Egypt in 2021," *EgyptToday*, February 2019; "Egypt's Sisi Approves Establishment of Russia Industrial Zone," *Middle East Monitor*, February 1, 2019.

127 "IMB Piracy Report 2018: Attacks Multiply in the Gulf of Guinea," *International Chamber of Commerce*, January 2019.

the EU will have to deal with China on other issues as well, such as export controls and defense cooperation in the sphere of stability missions.¹²⁸

2.4.3 EU dependency on energy and raw materials

With the construction of the Nord Stream 2 gas pipeline at an advanced stage, the debate surrounding the commercial and geopolitical implications is heating up, as the EU is becoming more aware of the risks. The debate highlights tensions within the EU and NATO. Germany's role as an advocate of Nord Stream 2 has been heavily criticized, by Poland, for example. The European Parliament adopted a resolution urging Germany to halt the project. Proof of heightened geopolitical tensions can also be found in US policy, with preparations to sanction EU firms (co-)financing Nord Stream 2. This could potentially also hurt Dutch firms. Another source of debate is the Baltic region. In January, Russia launched a liquid natural gas (LNG) power plant in order to make its Kaliningrad exclave self-reliant if NATO members unplug the power grid. The exclave is at risk of becoming the stage for a new gas 'Cold War'.¹²⁹

An area particularly prone to geopolitical tensions is the Arctic region, where both China and Russia are expanding their presence. China has announced that it will start building its first airport in the Arctic. Russia has given the state corporation Rosatom a leading role in the development of the Northern Sea Route. The company recently opened a base in Murmansk to monitor and regulate ship traffic. Russia is also renewing and reactivating Cold War military infrastructure in the Arctic. China and Russia are increasingly seeking cooperation in the region. China is seeking to integrate its 'Polar Silk Road' – a predominantly Sino-Russian partnership – into the greater BRI. A major component is the development of joint ventures with Russia in resource extraction, including fossil fuels and raw materials. China will likely gain more from their collaboration, as Russia's ventures are too reliant on stable oil prices.¹³⁰

128 Paola Tamma, "Italy Signs up to China's Massive Infrastructure Project," *POLITICO*, March 23, 2019; Tarmo Virki, "China's Touchstone to Invest \$17 Billion in Helsinki-Tallinn Tunnel," *Reuters*, March 8, 2019; Philippe Le Corre, "China's Golden Era in Portugal," Carnegie Endowment for International Peace, November 24, 2018; Mads Frese, "Italy Takes China's New Silk Road to the Heart of Europe," *EUobserver* (blog), March 2019.

129 Jo Harper, "Kaliningrad Gets Moscow Energy Boost as Baltic States Pull Plug," *DW.COM*, March 22, 2019; Michael Nienaber, "U.S. Warns German Companies of Possible Sanctions over Russian Pipeline," *Reuters*, January 13, 2019; Dominik Istrate, "Nord Stream 2 must be stopped, EU parliament says," *Emerging Europe*, March 14, 2019; "US Moves Ahead on Nord Stream 2 Sanctions," *EUobserver*, March 2019.

130 Malte Humpert, "China Launches Domestically-Built 'Xue Long 2' Icebreaker," *High North News*, September 11, 2018; Nastassia Astrasheuskaya, "Russia Gives Nuclear Group Control of Arctic Sea Route," *Financial Times*, December 13, 2018; Trym Aleksander Eiterjord, "China's Busy Year in the Arctic," January 2019; Donald Gasper, "China and Russia Want to Develop Arctic Energy Resources Together, and US Disapproval May Not Deter Them | South China Morning Post," *South China Morning Post*, September 2018.

The energy sector has also become increasingly vulnerable to cyber threats. In addition, AI-based malware will likely usher in a new era of threats to the energy industry, allowing hostile actors to wreak havoc on a scale hitherto unknown. AI-driven malware can be employed with unprecedented accuracy and is very hard to stop.¹³¹

2.4.4 Economic espionage

Although China has been conducting espionage for years, it is currently ramping up its espionage activities. In particular, the number of corporate cyberattacks outside China has recently soared and costs have risen accordingly. The Netherlands' General Intelligence and Security Service (AIVD) has called China "the biggest threat when it comes to economic espionage."¹³² China is particularly interested in Dutch companies that operate in the high-tech, energy, maritime, and life sciences and health sectors. A particularly concerning development is that China's Ministry for State Security (MSS) is working more closely with Chinese enterprises and uses cover organizations such as universities, trade associations, and think tanks. China has become more aggressive and seems to care less if it gets caught or if people go to jail. It also uses non-cyber means of espionage, such as recruiting employees to steal information or stealing specific technological inventions (for example, genetically modified rice seeds). These developments show how active China has become in the field of espionage.¹³³

Overall, it can be said that our economic prosperity – essentially dependent on preventing trade tensions, keeping trade routes open, ensuring the supply of energy and raw materials, and countering economic espionage – is under threat, not least from China. Moreover, these threats to free trade, access to energy and raw materials, and our competitive advantage in the fields of knowledge and technology, are expected to intensify over the coming years.

131 Lukas Trakimavičius, "The Threat of AI to Energy Security," RealClearDefense, December 7, 2018; Steve Ranger, "Cyberattacks: China and Russia Can Disrupt US Power Networks Warns Intelligence Report," *ZDNet*, January 2019; Gils, van, S, "Deltawerken En Sluizen Kwetsbaar Voor Cyberaanvallen," FD.nl, March 2019.

132 "AIVD Annual Report 2018 - Annual Report," May 14, 2019, 9.

133 Ellen Nakashima and David Lynch, "U. S. Charges Chinese Hackers in Alleged Theft of Vast Trove of Confidential Data in 12 Countries," *MSN*, December 21, 2018; Gordon Corera, "Looking for China's Spies," *BBC News*, December 2018; "AIVD Annual Report 2018 - Annual Report"; Scott Stewart, "A Sting Operation Lifts the Lid on Chinese Espionage," *Stratfor* (blog), October 2018.

2.5 CBRN Weapons

Over the past few years, chemical, biological, radiological, and nuclear (CBRN) weapons have returned to the forefront of the international political agenda. In particular, nuclear weapons and the discussions surrounding the related arms control regimes have been the center of attention. Not surprisingly, the results of our horizon scan are not very reassuring when it comes to the current trends and developments regarding CBRN weapons. Most of the threat-related trends in this field show a negative dynamic, which means that the threat is expected to become even more severe in the coming years (see Table 6).

2.5.1 Arsenals

A key trend in the CBRN domain is the fact that all nuclear-armed states are investing heavily in the modernization of their nuclear arsenals as well as in developing new missile technologies. Some of them are producing, and maybe even testing, low-yield nuclear weapons. The production of these weapons is controversial, as several experts argue that, with their lower (political) threshold for use, they raise the escalation potential. Moreover, experts speak of a growing arms race between the great powers

Table 6 CBRN weapons, multi-factor threat estimate (up to 2025)

Trends	Indicator	
Arsenals	Number of CBRN weapons	—
	Investments in modernisation of weapons	▲
	Investments in missiles	▲
Policies	Political threshold for CBRN weapon use	▼
	Non-state actors' access to CBRN weapon technology	▲
	Clear lines between CBRN and conventional weapons	▼
	Trust in multilateral system regarding CBRN	▼

■ Decreasing threat ■ Increasing threat
▲ Upward ▼ Downward — Net-zero / Stable

over hypersonic missiles. These missiles raise the escalation potential, due to the limited response time available to political and military actors when they are deployed, and because of the difficulty of distinguishing between nuclear-armed and conventionally armed ballistic and cruise missiles.¹³⁴

A second trend is that developments in biotechnology raise the risk of (terrorist) attacks with biological agents. Techniques such as Clustered Regulatory Interspaced Short Palindromic Repeats (CRISPR) allow for unprecedented precision in gene editing. While such techniques can be used to cure diseases, they can also be used to create new diseases or to modify existing ones.

A third trend that warrants mentioning here is the dual-use nature of new pharmaceutical applications, which makes future verification of arms control agreements and export control regulations more difficult.¹³⁵

2.5.2 Policies

Non-state actors have increased access to knowledge and technologies essential to the production of biological and chemical weapons. Controlling the spread of emerging technologies, such as additive manufacturing, 3D printing, and AI, which can be used to manufacture biological weapons, is difficult due to their dual-use nature. A similar trend can be witnessed in the field of chemical science. The lack of knowledge on the part of policymakers and the limited coverage of current regulatory regimes make it difficult to address the risks.¹³⁶

134 William J. Broad and David E. Sanger, "Race for Latest Class of Nuclear Arms Threatens to Revive Cold War," *The New York Times*, April 16, 2016, sec. Science; "Modernization of World Nuclear Forces Continues despite Overall Decrease in Number of Warheads," *SIPRI* (blog), June 17, 2019; John Borrie, Amy Dowler, and Pavel Podvig, "Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control," *UNODA* (blog), February 2019; "US Nuclear Weapons: First Low-Yield Warheads Roll off the Production Line," *The Guardian*, January 28, 2019, sec. World news; Douglas Barrie, "Trends in Missile Technologies," *IJSS* (blog), March 2019; R. Jeffrey Smith, "Hypersonic Missiles Are Unstoppable. And They're Starting a New Global Arms Race," *The New York Times*, June 19, 2019, sec. Magazine; Fei Su and Ian Anthony, "Reassessing CBRN Threats in a Changing Global Environment," *SIPRI* (blog), June 2019.

135 Fei Su and Ian Anthony, "Reassessing CBRN Threats in a Changing Global Environment."

136 Brockmann, K, Bauer, S, and Boulanin, V, "Arms Control and the Convergence of Biology and Emerging Technologies" (SIPRI, March 2019); Peter Dockrill, "Chilling New Research Shows How Dire a Smallpox Bioterror Attack Could Actually Get," *ScienceAlert*, February 2019; Shambhavi Naik, "Biological Weapons: The Impact of New Technologies," *CBW Magazine* (blog), June 2019; "How Emerging Technologies Increase the Threat from Biological Weapons," *World Economic Forum* (blog), March 2019. Fei Su and Ian Anthony, "Reassessing CBRN Threats in a Changing Global Environment."

Recent trends highlight the development of new weapon systems that make the distinction between nuclear and conventional weapons more diffuse. These more advanced systems make it difficult for states to determine whether an incoming weapon has a nuclear or conventional charge. This results in an increasingly blurred line between nuclear and conventional weapons, which could potentially lead to a nuclear war, as misperceptions may occur more easily. This risk is even more worrisome considering the entanglement of nuclear and conventional command and control (C2) systems.¹³⁷

Overall, our analysis of the trends and developments related to both arsenals of and policies regarding CBRN weapons warrants the conclusion that this particular issue will likely stay at the forefront of the international political agenda for years to come.

2.6 Terrorism

Terrorism has been on the international political agenda for years now. And while the nature of terrorism itself may not have changed, terrorists have proven to be quite inventive when it comes to their choice of methods for attack and for recruitment. This leads to the question of whether the character of terrorism is changing, by utilizing or weaponizing technology. To explore the ways in which technology impacts the threat, we have undertaken a horizon scan looking at trends in terrorism and technology (Table 7). Based upon our horizon scan, the most important trends and developments imply that the corresponding threats related to terrorism and technology have intensified. It should be noted, however, that these trends are often interlinked and cannot be seen separately. In the section below, we therefore specifically focus on the nexus between the two.

137 Downman, M and Messmer, M, “Re-Emerging Nuclear Risks in Europe: Mistrust, Ambiguity, Escalation and Arms-Racing between NATO and Russia” (The British American Security Information Council, April 2019); James M. Acton, “Why Is Nuclear Entanglement So Dangerous?,” Carnegie Endowment for International Peace, January 2019; Michael T. Klare, “An ‘Arms Race in Speed’: Hypersonic Weapons and the Changing Calculus of Battle,” June 2019; James Acton, “The Weapons Making Nuclear War More Likely,” *BBC News*, February 2019.

Table 7 Terrorism, multi-factor threat estimate (up to 2025)

Trends	Indicator	Trend
Trends in terrorism	Number of terrorist attacks worldwide	▲
	Number of terrorist attacks in Europe	▲
	Number of terrorist attacks involving drones worldwide	▲
	Use of modern communication technology in terrorist activity	▲
Trends in technology	Access to technology	▲
	Connectedness of systems	▲
	Proliferation of AI	▲
	Proliferation of drone technology	▲
	Technology control and regulation	▲

■ Decreasing threat	■ Increasing threat
▲ Upward	▼ Downward — Net-zero / Stable

2.6.1 Use of modern technology in terrorist activity

Faced with an increase in censorship by mainstream social media, such as YouTube, Facebook, and Twitter, extremists are looking for alternatives. IS, for example, has been diversifying its output channels, in part by spreading content through lesser known portals. A fragmentation of jihadist propaganda has been witnessed, which may make it more difficult to reach the target audience, but also harder to control.¹³⁸

Cryptocurrencies could prove an attractive way to finance (terrorist) attacks. Terrorists have a particular incentive to crowdfund with Bitcoin over other cryptocurrencies that have fewer users and a more cumbersome exchange process. However, Bitcoin still does not have much purchasing power, nor does it provide the necessary anonymity, as it

138 Laurence Bindner and Raphael Gluck, "Trends in Islamic State's Online Propaganda: Shorter Longevity, Wider Dissemination of Content," *ICCT*, December 5, 2018; "Terrorism Situation and Trend Report 2019," Europol, June 2019; Rita Katz, "A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps," *Wired*, January 9, 2019; "Analysis: The Use of Open-Source Software by Terrorists and Violent Extremists," *Tech Against Terrorism* (blog), 2019; Megan Squire, "Can Alt-Tech Help the Far Right Build an Alternate Internet?," *Fair Observer* (blog), July 23, 2019.

requires connecting to a bank account. So, for now, cash remains king in the world of terror financing. Nevertheless, if cryptocurrencies become more anonymous, they might provide a valid – and hard-to-track – alternative.¹³⁹

2.6.2 Connectedness of systems

As the connectedness of infrastructural systems increases further, so does the risk of cyberattacks on critical infrastructure (e.g., transport networks, energy grids, hospitals, etc.). For now, terrorists have limited internal capabilities to conduct the technologically complicated cyberattacks necessary to impact critical infrastructure. However, the Dark Web provides them with the option to buy readily available tools to conduct low-level cyberattacks themselves. The Dark Web even provides the opportunity to ‘buy attacks’, which are then conducted by professional hackers. These hackers are not necessarily sympathetic to a terrorist cause, but just in it for the money. IS sympathizers have already demonstrated their willingness to buy cyberattack tools and services from the digital underworld, which could potentially severely affect our national security.¹⁴⁰

2.6.3 Proliferation of AI-driven technology

A key pattern can be identified when looking at, for example, the use of social media, encryption technology, and drones over time: when a consumer technology becomes widely available, terrorists will look for ways to adapt it for their own purposes. AI will almost certainly end up fitting into this pattern. Experts warn about a variety of high-level threats, including “swarms of killer drones,” “self-driving vehicles carrying car bombs and conducting ramming attacks,” or “AI-enabled assassinations.” But AI also provides terrorist organizations with a plethora of more likely, low-level (non-lethal) means, including AI capabilities for intelligence purposes (e.g., AI-enabled social network mapping), deep fakes as a PSYOPS tool, or AI-based extortion.¹⁴¹

139 Brenna Smith, “The Evolution Of Bitcoin In Terrorist Financing,” *Bellingcat* (blog), August 9, 2019; Eva Entenmann, “Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?,” *ICCT*, November 1, 2018; Catherine De Bolle, Executive, “Internet Organised Crime Threat Assessment 2018,” Europol, 2018; Cynthia Dion-Schwarz, David Manheim, and Patrick B. Johnston, “Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats,” Product Page (RAND Corporation, 2019).

140 Beatrix Immenkamp et al., “The Fight against Terrorism” (European Parliament, June 2019); Ilan Berman, “Technology Is Making Terrorists More Effective—And Harder to Thwart,” *The National Interest*, February 22, 2019.

141 Seth Harrison, “Evolving Tech, Evolving Terror” (CSIS, March 2018); Cat Cronin, “Weaponizing Technology: 21st Century Terrorism,” American Security Project, June 2019; Daveed Gartenstein, “Terrorists Are Going to Use Artificial Intelligence,” *Defense One*, May 2018; Larry Johnson, “Automated Cyber Attacks Are the Next Big Threat. Ever Hear of ‘Review Bombing’?,” *Entrepreneur*, December 21, 2018.

Putin has stated that he believes the ‘winner’ of the AI arms race “will be ruler of the world.”¹⁴² As the most powerful states in the world engage in an AI arms race, small rogue states and terrorist actors can potentially profit from this interstate competition. Experimenting with machine learning technology and AI will not be the preserve of nation-states. Terrorists will be able to access advanced AI technologies through the open market or the black market and exploit these for nefarious purposes, as they already have done with end-to-end encryption, social media, virtual currencies, and unmanned aerial systems (drones).¹⁴³

2.6.4 Proliferation of drone technology

One of the most concerning developments in the area of terrorism and technology is the increasing attractiveness of the use of drones. Increasingly, off-the-shelf drones are able to carry heavier payloads, fly and loiter for longer periods of time, venture farther from their controller, and possess more secure communications links. This has not escaped the attention of terrorist groups. Although drones have been used to carry explosives in the past few years in combat zones, the West has been spared such attacks. This, however, may not last. IS propaganda posters have already depicted drone attacks on the Eiffel Tower in Paris and in New York City.¹⁴⁴ Protective measures against drone attacks are currently very limited, certainly in public spaces. Moreover, if terrorists succeed in staging an attack by using drones, the psychological impact on our sense of security will likely be significant.¹⁴⁵

2.6.5 Technology control and regulation

Lastly, with technologies developing at an ever increasing speed, keeping up our understanding of the many ways in which these technologies might signify a threat is challenging. In the aftermath of the 9/11 attacks, the 9/11 Commission identified various red flags that had been noticed before the attack but were disregarded because of a failure of imagination – a failure to imagine that someone could get on a plane, turn that plane into a weapon, and fly it into a building. In recent years, we have seen multiple failures in imagination as analysts tried to discern what terrorists would do with emerging technologies, including cyber and AI. As technology is developing

142 Ryan Daws, “Putin Outlines Russia’s National AI Strategy Priorities,” *AI News* (blog), May 31, 2019.

143 Daveed Gartenstein, “Terrorists Are Going to Use Artificial Intelligence.”

144 Warrick, “Use of Weaponized Drones by ISIS Spurs Terrorism Fears,” *The Washington Post*, February 2017; Zak Doffman, “Warning Over Terrorist Attacks Using Drones Given By EU Security Chief,” *Forbes*, August 2019.

145 Warrick, “Use of Weaponized Drones by ISIS Spurs Terrorism Fears”; Doffman, “Warning Over Terrorist Attacks Using Drones Given By EU Security Chief.”

exponentially, it is becoming increasingly difficult to identify and prepare for different potential threats, let alone to control and regulate the use of various new technologies.

Overall, new technologies and the increasing availability of these technologies to terrorists are expected to provide them with potential new methods, both to stage their attacks and to recruit and inspire followers. In particular, drones are becoming more powerful and complex, which makes them increasingly attractive for legitimate use, but potentially also for hostile acts. It is expected that off-the-shelf drones will be able to carry ever heavier payloads, fly and loiter for longer, venture farther afield from their controllers, and be able to do so via more secure communications links. Continuous monitoring is therefore needed to keep up with the potential threats posed by these rapidly developing technologies.

2.7 Sub-conclusions

The trends and developments in the six fields of military competition, cyber security, hybrid conflict, economic security, CBRN weapons, and the nexus between terrorism and technology show a predominantly negative picture. Moreover, with regard to these six topics, most of the indicators for the next five years point to an increased threat.

Military competition is increasing. The security perceptions of major military powers are worsening. The use of military threats is rife in the exchanges between rival states across the globe. Global net defense expenditures have grown only marginally over the last ten years, but the defense budgets of certain major powers have increased significantly – even doubling, in the case of China. Funds dedicated to military R&D and the modernization of armed forces by harnessing technologies such as AI and unmanned systems are increasing across the board. Conflicts have diversified. While traditional interstate conflict remains rare, we have seen a clear accretion in the number of internationalized intrastate conflicts since the beginning of this century.

Cyber security has also intensified in recent years. The number of cyber-enabled espionage and computer network attack incidents has increased. Disinformation campaigns have become mainstream. States are boosting their cyber-military as well as cybersecurity budgets. Our analysis of the intentions, capabilities, and activities suggests that cyber conflict is unlikely to level off in the near future, with considerable risks of escalation.

Similarly, hybrid conflict has become more salient. Although by definition impossible to fully demarcate, the use of hybrid tactics is proliferating, with more frequent deployment of proxy actors across different geographical theaters, regular aerial and maritime

territorial intrusions, attempts to exert influence over foreign democratic processes, and growing resort to economic coercion which has important cross-overs to economic security.

In the field of economic security, it is our economic prosperity that is under threat, not least from China. Moreover, free trade flows, guaranteed access to energy and raw materials, and maintaining our competitive advantage in the fields of knowledge and technology in light of economic espionage are all expected to remain under pressure over the coming years.

With reference to CBRN weapons, states are expected to continue to invest in both the modernization of their nuclear arsenals and in hypersonic missiles. At the same time, the lines between CBRN and conventional weapons will probably become increasingly blurred. Non-state actors could more easily gain access to CBRN weapons technology. It is developments like these that warrant the conclusion that this particular issue will probably stay at the forefront of the international political agenda for years to come.

Finally, with regard to terrorism, drones are expected to become more powerful and smarter, making them increasingly attractive for the perpetration of hostile acts. Off-the-shelf drones will probably be able to carry ever heavier payloads, fly and loiter for longer, venture farther afield from their controllers, and be able to do so via more secure communications links. It is these developments, coupled with the risk of proliferation to non-state actors, that are most worrying.

3 Development of the International Order

Significant developments are taking place in the collection of regimes that together constitute the international order regulating state interactions in particular domains. This chapter highlights the most important developments across the most important regimes for the six threat themes from the Dutch *Integrated Foreign and Security Strategy 2018-2022*.¹⁴⁶

3.1 Military Competition

The increase in military competition coincides with an overall weakening of arms control regimes. In particular, the norms and rules pertaining to the non-proliferation of nuclear weapons and technology control of associated delivery vehicles face erosion. Several international treaties, like the Nuclear Non-Proliferation Treaty (NPT) of 1970, aim to mitigate the destabilizing effect of arms races through the introduction of standards and verification mechanisms.¹⁴⁷ These treaties are supplemented by other international initiatives that contain confidence-building measures to constrain military competition, such as the Open Skies Treaty (OST) of 1992,¹⁴⁸ the Vienna Document in 1990,¹⁴⁹ and the Wassenaar Arrangement from 1995.¹⁵⁰ Our analysis of the health of the international legal framework governing military competition finds that this framework faces significant erosion, with negative trends evident both in the degree to which states break the rules upon which it rests and in the infallibility of the norms that underpin those rules (see Table 8).

146 See for the more extensive research on these topics the following papers: Sico van der Meer, Danny Pronk, and Adája Stoetman, "CBRN Weapons: Where Are We in Averting Armageddon?" (Clingendael, November 5, 2019); Adája Stoetman and Minke Meijnders, "Economic Security with Chinese Characteristics," Clingendael, November 2019.

147 See "Treaty on the Non-Proliferation of Nuclear Weapons (NPT)," United Nations Office for Disarmament Affairs (UNODA), 1970; "The Arms Trade Treaty," The Arms Trade Treaty, 2018.

148 Daryl Kimball, "The Open Skies Treaty at a Glance," Arms Control Association, October 2012.

149 "Ensuring Military Transparency – the Vienna Document," Organization for Security and Co-operation in Europe (OSCE), accessed September 19, 2019.

150 "The Wassenaar Arrangement," Wassenaar, accessed September 19, 2019.

Table 8 Military competition, multi-year regime estimate (up to 2025)

Norms	Trend
States ought not to use or develop nuclear weapons	▼
States ought to adhere to conventional arms control regimes	—
States ought not to engage in threatening behavior	▼
States ought to respect territorial sovereignty and inviolability	—

Rules	Trend
The degree to which states comply with international law as codified in treaty and/or customary and/or domestic law in the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), the Intermediate-range Nuclear Forces (INF) treaty, UN Chapter VII Resolutions 1540 and 1977, the New Strategic Arms Reduction Treaty (New START; US and Russia).	▼
The degree to which states comply with regimes such as the Nuclear Suppliers Group, the Zangger Committee, the International Atomic Energy Agency (IAEA), UNSC Resolution 1540.	▼
The degree to which states comply with international law such as set out in the Protocol I to the Geneva Conventions of 1977 Art. 36, the Open Skies Treaty, the Treaty on Conventional Armed Forces in Europe (CFE), the Arms Trade Treaty, Vienna Document.	▼
The degree to which states comply with regimes and confidence-building measures, including the Wassenaar Arrangement, Missile Technology Control Regime (MTCR), the UN Register of Conventional Arms (UNROCA), and Guiding Principles by the 2018 Group of Governmental Experts on Lethal Autonomous Weapons (LAWS).	▼
The degree to which states comply with Art. 2(4) of the UN Charter, in which states have agreed to refrain from threat or use of force.	—
The degree to which states comply with not only Art. 2(4) of the UN Charter, but also with the articles pertaining to lawful intervention as can be declared by the UN Security Council (in compliance with – among others (but first and foremost) – Arts. 1, 39, 51, as well as states' compliance with agreements such as the (non-binding) Helsinki Final Act.	▼

■ Decreasing threat ■ Increasing threat
▲ Upward ▼ Downward — Net-zero / Stable

3.1.1 States ought not to use or develop nuclear weapons

The past decade has seen an erosion of nuclear arms control regimes and the norms that underpin them. This regulatory framework can be understood as splitting between measures relating to nuclear non-proliferation and controls on the development and deployment of delivery vehicles (arms control). At the macro level, all of the relevant treaties exhibit a consistent downward trend in compliance. The result is an erosion of both the regulatory framework (the rules) and the normative framework (the norms) that underpin it. This can be partially attributed to the outdated nature of several of the key bilateral treaties within this domain, but also to the fact that military competition is driving the development of new nuclear weapons and delivery vehicles.

Several trends point toward an erosion of the rules underpinning the norm that states ought not to use or develop nuclear weapons. Technically speaking, the NPT has not been breached. However, the activities undertaken by Iran and North Korea in continuing the development of nuclear weapons and nuclear delivery vehicles, despite the fact that North Korea is not a signatory of the NPT, mark negative developments for the non-proliferation regime. Although trends in compliance with the rules of the NPT are therefore neutral 'on paper', they are, in effect, under pressure. Of equal concern are the developments with respect to the Intermediate-Range Nuclear Forces Treaty (INF) and the New Strategic Arms Reduction Treaty (New START). The INF's dissolution has apparently created a domino effect, which now threatens the New START extension. Its potential future abandonment by the US and Russia – the world's foremost nuclear powers – constitutes a strong indicator of the erosion facing the rules-based order enforcing nuclear arms control.

Furthermore, many of the relevant multilateral agreements are thin and limited. Limited because they do not cover nuclear weapons of non-signatories or their means of delivery; and thin because they lack verifiable compliance mechanisms. Treaties such as the New START were originally designed for a bipolar world. Today, China is developing and strengthening its nuclear arsenal, while Pakistan and India are updating their nuclear capabilities as key components of their strategic defensive posture.¹⁵¹

The norm that states ought not to develop nuclear weapons is also eroded by the development of new technologies, including air-launched and boosted-glide weapons, second-generation multiple independently targetable re-entry vehicle (MIRV) capable missiles, nuclear-powered intercontinental ballistic missiles (ICBMs), and low-yield and variable-yield nuclear weapons. The development of these technologies is not explicitly

151 Wu Riqiang, "Trilateral Arms Control Initiative: A Chinese Perspective," *Bulletin of the Atomic Scientists* (blog), September 4, 2019; Alexey Arbatov, "Mad Momentum Redux? The Rise and Fall of Nuclear Arms Control," *Survival* 61, no. 3 (May 4, 2019): 7–38.

prohibited under the existing agreements,¹⁵² but often results in the introduction of dynamics that undermine the spirit of existing security structures. Hypersonic missiles travelling at speeds surpassing Mach 5 are much more difficult to track and shoot down using conventional air defense systems.¹⁵³ They thus undermine states' second-strike capabilities, a key tenet of the existing nuclear power balance. This highlights the need for more comprehensive regulations, not just on the quantity of nuclear stockpiles, but also on the delivery vehicles that accompany them. All of this yields a negative appraisal of the overarching norm that states ought not to use or develop nuclear weapons. This assessment is supported by the Bulletin of the Atomic Scientists' Doomsday Clock, which has observed a negative trend since 2010, warning that "it's still two minutes to midnight."¹⁵⁴

3.1.2 States ought to adhere to conventional arms control regimes

The regime regulating the non-proliferation of conventional arms also faces erosion. Rules included in this analysis are Article 36 (Protocol 1, Geneva Convention), the Open Skies Treaty (OST), the Treaty on Conventional Armed Forces in Europe (CFE), the Arms Trade Treaty (ATT), and the Vienna Document. An analysis of developments affecting the Wassenaar Arrangement, the Missile Technology Control Regime (MTCR), The Hague Code of Conduct against Ballistic Missile Proliferation, the UN Register on Conventional Arms (UNROCA), and the Guiding Principles formulated by the 2018 Group of Governmental Experts (GGE) on Legal Autonomous Weapons (LAWS) is also included. Trends within these treaties show a consistent decrease in compliance, with the result being an erosion of the regulatory framework. The trend is neutral on the normative side. This is largely the result of the fact that states, despite their reluctance to observe the compliance verification mechanisms, tend to remain within the relevant international treaties.

3.1.3 Assessment of the state of the conventional arms control regime

With regard to adherence to and compliance with conventional arms regimes, we observe mixed developments. Over the past ten years we have seen a rise in formal adherence, i.e., signatures and ratifications of rules governing this behavior, as well as – in some areas – the expansion of certain treaties and regimes. This is balanced by two negative developments. First and foremost, the strained US–Russia relationship has undermined the integrity of trend-setting agreements such as the OST and the

152 Arbatov, "Mad Momentum Redux?"

153 As evidenced by Moscow's push to develop these weapons specifically to counter the impact that US air defenses have on Russia's nuclear deterrent. See Michael T. Klare, "An 'Arms Race in Speed': Hypersonic Weapons and the Changing Calculus of Battle."

154 Bulletin of the Atomic Scientists, "Doomsday Clock - Timeline," *Bulletin of the Atomic Scientists* (blog), 2019.

Treaty on Conventional Armed Forces in Europe. Second, virtually all treaties containing compliance measures,¹⁵⁵ as opposed to mere formal adherence provisions, have exhibited significant deterioration. Take for instance the Arms Trade Treaty: although an increasing number of states pledges to adhere to the underlying rationale of the treaty, the number of submissions of the mandatory reports has plunged.

Nevertheless, there is no indication of declining adherence to the norm according to which control of the development, transfer, and use of conventional arms is desirable. There are two reasons for this. First, the individual regimes and documents explored in this analysis show meaningful efforts at incorporating new technologies. Despite the fact that the world's great powers are often accused of stalling and manipulating negotiations,¹⁵⁶ several positive developments offer some grounds for optimism. These include the ratification of the new Joint Declaration for the Export and Subsequent Use of Armed or Strike Enabled Unmanned Aerial Vehicles of 2016, the mere fact that discussions regarding the legality of LAWS are ongoing, and the MTCR's possible future inclusion of slow-flying UAVs. Second, the vocal condemnation of deteriorations relating to the trust-building and verifications mechanisms speaks to the presence of an international community that continues to value the basic principle of the norm.¹⁵⁷ Increases in adherence to the Wassenaar Arrangement and the Hague Code of Conduct against Ballistic Missile Proliferation also contribute to the norm's neutral appraisal, as they indicate that – although the rules are being complied with less consistently – states still place value in the notion that the trade in conventional arms should be regulated at the international level.

3.1.4 States ought not to engage in threatening behavior

The norm that states ought not to engage in threatening behavior is codified in international law, namely Article 2(4) of the UN Charter, which states that “all members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner

155 Except for the CCW.

156 China has refused to ratify or comply with any limitations on the development and production of autonomous weapons and the US and Russia both oppose any ban whatsoever. See “Could China Develop Killer Robots in the Near Future? Experts Fear So,” *Time*, accessed October 31, 2019. See also “Country Views on Killer Robots” (Campaign To Stop Killer Robots, November 22, 2018).

157 See for example NATO's and OSCE's reaction to Russia's withdrawal from CFE Treaty, the latter labeling it a “dangerous move” and the former a “step in the wrong direction” (see “Russia's Withdrawal from CFE Treaty Work a ‘dangerous Move,’ Says OSCE PA Security Chair | OSCE,” accessed October 16, 2019; “NATO: Suspension of Treaty Is Step in Wrong Direction - World News - Jerusalem Post,” accessed October 23, 2019; “The Secretary General's Annual Report 2015” (NATO, 2015).

inconsistent with the Purposes of the United Nations.”¹⁵⁸ The rules underpinning this norm have faced no significant decrease in compliance over the past ten years, but the norm itself has been eroded. The assessment of a stable rule is based on the fact that, while states frequently violate this norm by threatening one another,¹⁵⁹ the volume and intensity of this threatening behavior have not increased significantly at the global/system level over the past decade. The norm is conceptualized as facing erosion largely because the advent of hybrid tactics has allowed states to actively pursue objectives which run contrary to it without infringing on it in the formal sense.

Our analysis has focused on the threat of force rather than on the actual use of force, and it relies on expert judgment, supplemented by ICEWS-derived data on the use of threats in interstate relations.¹⁶⁰ The quantitative analysis does not indicate that the rate of non-compliance has increased significantly over time, but does highlight a number of peaks in threatening verbal behavior. These include the tit-for-tat exchange of threats between the US and North Korea,¹⁶¹ Donald Trump’s letter to Turkish President Erdogan in which he threatened to “destroy the Turkish economy” in October 2019,¹⁶² Vladimir Putin’s nuclear sabre rattling,¹⁶³ back-and-forth coercive

158 “Charter of the United Nations,” August 10, 2015.

159 Thomas M. Franck, “Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States,” *The American Journal of International Law* 64, no. 5 (1970): 809–37.

160 The data-based component of the analysis incorporates a CAMEO-code-based methodology, which utilizes event data to code instances of likely Article 2(4) violations. This is operationalized by means of a measurement of international-level military threat issuances. As is also the case in the “intentions” section, data is derived by filtering for event 138 with the sub-codes 1381, 1382, 1384, 1385 within the ICEWS dataset. These codes refer to threats of military force (138), threats of blockade (1381), threats of occupation (1382), threats of conventional attacks (1384), and threats of unconventional mass violence (1385). See Philip Schrodt, “CAMEO Conflict and Mediation Event Observations Event and Actor Codebook” (Pennsylvania State University, 2012). This analysis distinguishes itself from the analysis included in Table 2 because – rather than gauging only the actions of the world’s most active and/or influential states (a measurement which is more prudent for gauging threat) – it incorporates a holistic (international) perspective (see Table 2).

161 Associated Press, “Donald Trump Threatens ‘Total Destruction’ of North Korea over Nuclear Programme during UN Address,” *South China Morning Post*, September 19, 2017; Kelsey Davenport, “Chronology of U.S.-North Korean Nuclear and Missile Diplomacy | Arms Control Association,” *Arms Control Association – Fact Sheets & Briefs*, October 2019.

162 Abbey Marshall, “Erdogan Says He Returned Trump’s Threatening Letter on Syria Invasion,” *POLITICO*, 2019.

163 “Putin to Trump: We’ll Develop New Nuclear Missiles If You Do,” *Reuters*, August 5, 2019.

messages and armed activities between Washington and Tehran,¹⁶⁴ and recurring military threats between Riyadh and Tehran.¹⁶⁵

Notwithstanding the lack of significant change within the rule, the norm associated with Article 2(4) is facing erosion because several important military powers have deployed military threats in a number of dangerous situations in recent years, thereby effectively changing the standards of the international discourse. This is further aggravated by the increased prevalence of gray zone operations. The latter negatively impact the norm, because they fall below the legal threshold of war.¹⁶⁶ Hybrid tactics such as cyber measures or informational operations exploit the lack of definition of “use of force” in Article 2(4), which is often associated with a particular “threshold of violence.”¹⁶⁷ The proliferation and normalization of hybrid tactics in state toolkits negatively impacts the norm, because these measures constitute a conscious effort to achieve objectives which are incompatible with the spirit of Article 2(4). State engagement in hybrid warfare and gray zone operations can thus generally be viewed as being indicative of a lack of subscription to the norm itself. Hence, the increasing presence of hybrid measures of coercion throughout the last ten years presents a negative trend in compliance with the norm discussed here.¹⁶⁸

3.1.5 States ought to respect territorial sovereignty and inviolability

Over the past decade, the rules pertaining to respect of territorial sovereignty have faced increasing erosion, whereas the norm has remained stable. That conclusion is based on a quantitative assessment of the number of state-on-state uses of violence, an examination of the legal opinions of relevant institutions, and the collection of a list of the actions and justifications employed by states whose activities may be seen as infringing on the intent of Article 2(4).

164 This rhetoric has become specifically agitated in the wake of a recent Iranian downing of a US RQ-4A Global Hawk. See Michael D. Shear et al., “Strikes on Iran Approved by Trump, Then Abruptly Pulled Back,” *The New York Times*, June 20, 2019, sec. World; Ann Gearan, “Trump’s Dual Instincts on Iran: Big Threats and an Eagerness to Deal,” *Washington Post*, 2019.

165 Patrick Wintour, “Iran Threatens ‘all-out War’ If Action Taken over Saudi Oil Strike,” *The Guardian*, September 19, 2019, sec. World news.

166 Hal Brands, “Paradoxes of the Gray Zone - Foreign Policy Research Institute,” *FPRI* (blog), February 5, 2016; Frank Bekkers, Rick Meessen, and Deborah Lassche, “Hybrid Conflicts: The New Normal?” (The Hague, Netherlands: TNO, December 2018).

167 Matthew C. Waxman, “Cyber Attacks as ‘Force’ under UN Charter Article 2(4),” *International Law Studies* 87, no. 1 (January 1, 2011): 5; “Independent International Fact-Finding Mission on the Conflict in Georgia,” 2009.

168 Bianca Torossian, Lucas Fagliano, and Tara Görder, “Global Security Pulse October 2019: Hybrid Conflict,” Strategic Monitor Program (The Hague, Netherlands: The Hague Centre for Strategic Studies, October 24, 2019).

Our analysis of state-on-state violence-related events – instances in which one state has employed conventional force (aerial weapons, blockades, CBRN weapons, etc.) against another state – shows a quantitative increase.¹⁶⁹ In combination with the tripling of the number of internationalized intrastate conflicts over the past decade, this corroborates the notion that the rule pertaining to the actions-based portion of Article 2(4) is facing significant erosion. This finding is not mirrored in trends pertaining to international institutions' judgments, largely because of the nature of these institutions or their internal (political) deadlocks.¹⁷⁰ An analysis of the International Court of Justice's (ICJ) and United Nations Security Council's (UNSC) declarations shows no uptick in the occurrence of judgements and condemnations of unlawful state-on-state violence.¹⁷¹ The ICJ was predominantly solicited to resolve disputes related to border delineation, often regarding maritime access,¹⁷² while the UNSC, despite acknowledging certain "threats to peace," has not once noted an outright breach of UN Charter Article 39 – and, by extension, Article 2(4) – with respect to territorial integrity.¹⁷³

An examination of states' justification of noteworthy instances of interventionism indicates continued relevance of the norm. States continue to feel the need to justify their behavior, e.g., by citing legal precedents or by securing invitations from the host

169 This trendline is synthesized on the basis of CAMEO codes 190, 191, 192, 194, 195, 200, 204 within the ICEWS dataset. These respectively refer to instances of the use of conventional force (190) – a "blanket" code which covers instances ranging from the use of aerial weapons (195) to territorial occupation (192). Codes 200 and 204 refer to instances in which CBRN weapons are used against state actors. See Schrodt, "CAMEO Conflict and Mediation Event Observations Event and Actor Codebook."

170 In the case of the UNSC, the most glaring complication presents in the institution's politicization, which might preclude some infringements from being labeled as such. A similar shortcoming recurs in the case of the ICJ, which is unable to initiate proceedings on its own initiative.

171 The Permanent Court of Arbitration is closely related to this category of institutions and stands out as the organ ignored by China in its deliberation on the nine-dash line. (see Owen Bowcott, "Beijing Rejects Tribunal's Ruling in South China Sea Case," *The Guardian*, July 12, 2016, sec. World news.) Nonetheless, this institution solely resolves issues that stem from existing international agreements, and is therefore of a distinct and less authoritative nature than the two mentioned.

172 "List of All Cases | International Court of Justice," accessed October 23, 2019.

173 Article 39 stipulates that "The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security." For 2008–2009 see "Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter)" (United Nations, 2009 2008), for 2009–2011 see "Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter)" (United Nations, 2011 2010), for 2012–2013 see "Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter)" (United Nations, 2013 2012), for 2014–2015 see "Repertoire of the Practice of the Security Council" (United Nations, 2015 2014), and for 2016–2017 see "Repertoire of the Practice of the Security Council" (United Nations, 2017 2016).

government. This is visible in, among others, Turkey’s invocation of the right to self-defense under the UN Charter as justification for its intervention in Syria (2019);¹⁷⁴ the US-led coalition’s reference to resolution 2249 and its inclusion of an authorization to eradicate terrorism in Syria (2015);¹⁷⁵ Saudi Arabia’s going to great lengths to demonstrate the legality of its intervention in Yemen by invitation in what amounts in its view to an international attack (Iran’s support of rebels, 2015);¹⁷⁶ and Russia’s invocation of the right to self-determination and humanitarian intervention in both Ukraine (2014) and Georgia (2008),¹⁷⁷ recalling the precedent set by NATO’s intervention in Kosovo. Similarly, Article 51 on the right to self-defense was invoked over the reporting period by a great number of entities appearing in Annex II, including Azerbaijan,¹⁷⁸ Cambodia, Thailand,¹⁷⁹ Sudan, South Sudan,¹⁸⁰ Ukraine,¹⁸¹ India, and Pakistan.¹⁸² Conversely, no express contestation on the non-validity of the overarching norm can be observed among states. Albeit often depicted as deteriorating, our analysis therefore concludes that the norm of territorial sovereignty as a guiding principle of international relations remains functional.

174 “Turkey Justifies Syria Invasion by Claiming Right to Self-Defense under U.N. Charter,” *The Japan Times Online*, October 15, 2019.

175 David Cameron, “David Cameron’s Full Statement Calling for UK Involvement in Syria Air Strikes,” November 26, 2015, sec. News; “Yemen President Calls for UN Action,” *BBC News*, March 25, 2015, sec. Middle East.; See “Resolution 2249 (2015) Adopted by the Security Council at Its 7565th Meeting, on 20 November 2015” (United Nations Security Council, November 20, 2015).

176 Invitation by Hadi, see “Yemen President Calls for UN Action.”; officially stated connection between Iran and the rebels, justifying the intervention, see Dan Roberts Kareem Shaheen in Beirut and agencies, “Saudi Arabia Launches Yemen Air Strikes as Alliance Builds against Houthi Rebels,” *The Guardian*, March 26, 2015, sec. World news. and Jeremy M Sharp, “Yemen: Civil War and Regional Intervention,” *Congressional Research Service*, September 17, 2017, 17.

177 Georgia: “Statement by President of Russia Dmitry Medvedev,” President of Russia, accessed October 23, 2019.; Ukraine: Team of the Official Website of the President of Russia, “Address by President of the Russian Federation,” President of Russia, accessed October 22, 2019.

178 “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter),” 2009 2008; “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter)” (United Nations, 2013 2012); “Repertoire of the Practice of the Security Council,” 2017 2016; “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter),” 2013 2012; “Repertoire of the Practice of the Security Council” (United Nations, 2017 2016).

179 “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter)” (United Nations, 2011 2010).

180 “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter),” 2013 2012; “Repertoire of the Practice of the Security Council,” 2015 2014; “Repertoire of the Practice of the Security Council,” 2017 2016., “Repertoire of the Practice of the Security Council” (United Nations, 2015 2014) ; “Repertoire of the Practice of the Security Council,” 2017 2016.

181 “Repertoire of the Practice of the Security Council,” 2015 2014.

182 “Repertoire of the Practice of the Security Council.”

Overall, the conclusion seems warranted that the international regulatory framework of military competition is facing considerable setbacks, with an assortment of negative developments in the nature of compliance with the rules encapsulated in the regimes that make up this order, as well as in the infallibility of the norms that underpin those rules.

3.2 Cyber Security

International attempts to regulate activities in cyberspace have seen varying degrees of success. In 1998, Russia was the first country to introduce a resolution on information and telecommunications technology in the context of international security to the United Nations General Assembly.¹⁸³ Since 1998 the UN Secretary-General has submitted regular reports to the General Assembly on the views of member states on the issue. While it has become a settled principle that international law applies in cyberspace,¹⁸⁴ it is sometimes unclear when and, more specifically, how existing international law is to be interpreted and applied.

Establishing finely delineated legal responsibilities for the various regimes in cyberspace is often not possible. Indeed, legal agreements have proven to be difficult and time-consuming given definitional and ideological differences. Efforts within the UN have therefore focused on the development of norms:¹⁸⁵ voluntary, legally non-binding commitments that reflect a common standard of acceptable and prescribed behavior. These norms accompany and expand on existing legal understandings rather than attempting to craft new law, and are complemented by confidence-building measures: technical or practical measures that aim to enhance transparency, communication, and trust between actors. States' divergent views have led to a widening of schisms in multilateral fora on how international rules should be interpreted in the context of cyberspace,¹⁸⁶ at the same time as a number of core initiatives in the field of norm development have been taking root over the last couple of years.

183 UN General Assembly, "United Nations General Assembly Resolution 53/70" (United Nations, January 4, 1999), 70.

184 Harold H. Koh, "International Law in Cyberspace" (September 18, 2012).

185 United Nations Group of Governmental Experts, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98" (United Nations General Assembly, June 24, 2013).

186 United Nations General Assembly, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security A/RES/73/266" (United Nations, December 22, 2018); United Nations Group of Governmental Experts, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98."

The ability of governments to successfully manage the threat of major cyber conflict is hampered by the rapid development of digital technologies and the difficulties in attribution, but also by the dominant role of non-state actors, both as custodians and as disruptors. In cyberspace, governments represent only one of three stakeholder groups. There is also the private sector, which owns and runs most of its digital and physical assets, and civil society, which is largely responsible for coding and running the global Internet functions. The failure to make meaningful progress at the multilateral level has led non-state stakeholders to become more involved in developing rules of the road. Technological issues involved in regulating cyberspace are complex and the rapid pace of change calls for a more collaborative approach than ever before. Private institutions have therefore become engaged in developing policies that affect the markets and industries over which they preside, sometimes at their own initiative and sometimes in partnership with governments or civil society organizations.¹⁸⁷ Similarly, academia and the technical community have contributed by substantiating policy with more concrete or practical guidelines and solutions.¹⁸⁸

In the context of this complex, multi-stakeholder environment, our analysis of the development of (rather than compliance with) norms and rules on the protection of critical Internet infrastructure reveals a number of positive trends pertaining to the development and adoption of norms and rules, especially with regard to the protection of the public core of the Internet, the protection of critical infrastructure, and the protection of electoral infrastructure (see Table 9).

187 Policy initiatives of private organizations include Microsoft's calls for a Digital Geneva Convention, Digital Peace Now campaign and various norm proposals, the Siemens Charter of Trust, the Cybersecurity Tech Accord, and the World Summit on the Information Society (WSIS) Coalition. Perhaps the most prominent example of collaborative initiatives between governments, private institutions, and civil society organizations would be the Netmundial conference, whereas other examples would include the Internet Governance Forum and the recently launched Paris Peace Forum, which led to the Paris Call for Trust and Security in Cyberspace.

188 Guidelines and best practices can help develop a culture of security. National policies on information and network security are based on a multidisciplinary and multi-stakeholder approach. A culture of security cannot arise just out of technical solutions – a comprehensive approach is needed with socio-economic and legal considerations, and governments must therefore interact and engage with private and civil society actors. See Working Party on Information Security and Privacy, "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries" (Organisation for Economic Co-operation and Development, December 16, 2005).

Table 9 Cyber security, multi-year regime estimate (up to 2025)

Norms (Acceptance)*	Trend
The general integrity and availability of the public core of the internet should be protected	▲
Electoral infrastructure should be protected	▲
Non-state actors should not engage in offensive cyber operations	■
State critical infrastructure should be protected	▲

Rules	Trend
The degree to which state and non-state actors are adopting measures to protect the Public Core of the Internet (<i>Paris Call, GCSC, EU Cyber Security Act</i>).	▲
The degree to which state and non-state actors are adopting protective measures to advance article 2(4) of the UN Charter, which articulates this norm and elevates it as a principle of legal, and thus, binding character (<i>GCSC, United Nations Charter, Paris Call</i>).	▲
The degree to which states are adopting national regulation that prohibits private sector hack-backs (<i>Paris Call, GCSC Singapore Norm Package, US Active Cyber Defence Certainty Act</i>).	▼
The degree to which state and non-state actors are adopting measures to protect their critical infrastructure (<i>European Parliament NIS Directive, United Nations, UN GGE</i>).	▲

■ Decreasing threat	■ Increasing threat	
▲ Increase	▼ Decrease	■ Net-zero / Stable

3.2.1 Protecting the public core of the Internet

The relative success that norms can have in creating common ground among stakeholders is illustrated by the protection of the public core of the Internet. Responses to threats against the core Internet protocols and functions require the cooperation of states, the private sector, and civil society groups, as the Internet is privately owned and the infrastructure underpinning it governed and maintained by a community made up of individuals and civil society groups.¹⁸⁹ While the idea of protecting the core Internet functions has a longer history, the notion only recently became the subject of various norm proposals, most notably by the General Commission for the Stability of Cyberspace (GCSC)¹⁹⁰ and the Internet Society's Mutually Agreed Norms for Routing Security.¹⁹¹ The GCSC's proposal has since been accepted and adopted by several institutions, as manifested in its inclusion in the Paris Call for Trust and Security in Cyberspace¹⁹² and its adoption into law through the EU Cybersecurity Act.¹⁹³ The development of both a norm and rules for this particular issue is therefore positive.

3.2.2 The protection of national critical infrastructure

Another positive development is the degree to which state and non-state actors are taking measures to protect their critical infrastructure. Critical infrastructure can be defined as "systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of

189 A number of states openly insist that states should play a key role in governing Internet policy and the Internet's critical resources. Other states believe that efforts should be made to maintain what is generally referred to as the "multi-stakeholder model" of Internet governance, defined often as "a form of participatory and diverse form of governance", and try to keep discussions on Internet governance separate from discussions on international peace and security. See United Nations, "Cyberspace and International Peace and Security - Responding to Complexity in the 21st Century" (United Nations Institute for Disarmament Research (UNIDIR), 2017).

190 "Call to Protect the Public Core of the Internet" (The Global Commission on the Stability of Cyberspace (GCSC), 2017); "Definition of the Public Core" (The Global Commission on the Stability of Cyberspace (GCSC), 2018).

191 "Mutually Agreed Norms for Routing Security (MANRS) for Network Operators (ISP) and for Internet Exchange Points (IXP)," *Internet Society* (blog), accessed September 4, 2019; "Routing Security for Policymakers - An Internet Society White Paper" (The Internet Society, October 2018).

192 "Routing Security for Policymakers - An Internet Society White Paper."

193 The European Parliament and The Council of the European Union, "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)" (Official Journal of the European Union, April 17, 2019).

those matters.”¹⁹⁴ Recent events concerning national power grids as well as the extent to which automated systems are integrated with each other have led to fears that these systems may be susceptible to offensive cyber operations. Various efforts at the multilateral, regional, and national levels have aimed to address the issue of critical infrastructure protection – amongst them the GGE Report of 2015, which repeatedly emphasized the need to protect critical infrastructure and their associated information systems from ICT threats.¹⁹⁵ The United States Executive Order 13800¹⁹⁶ was aimed at improving the nation’s cyber posture and capabilities in the face of intensifying cybersecurity threats, while the National Institute of Standards and Technology issued a report on improving critical infrastructure cybersecurity.¹⁹⁷ The EU is undertaking its own efforts in this area,¹⁹⁸ and the Organization for Security and Co-operation in Europe (OSCE) has identified critical infrastructure protection as an important issue in its confidence-building measures as well as in other decisions.¹⁹⁹ Here too, the norm and rules development shows a positive trend.

3.2.3 The protection of electoral infrastructure

Civil society groups have extended the debate by focusing on elements of critical infrastructure that require specific attention, such as the technical infrastructure that

194 It has also been defined as “assets or systems which are vital for the maintenance of societal functions, health, safety, security, economic or social well-being of people.” In “EU Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection” (Official Journal of the European Union, December 8, 2008); James F. Sensenbrenner, “Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT),” Pub. L. No. H.R.3162 (2001).

195 United Nations Group of Governmental Experts, “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98.”

196 “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,” The White House, May 11, 2017.

197 “Framework for Improving Critical Infrastructure Cybersecurity” (National Institute of Standards and Technology, April 16, 2018).

198 The European Union Programme for Critical Infrastructure Protection (EPCIP) sets the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU states and in all relevant sectors of economic activity. See “Communication from the Commission on a European Union Programme for Critical Infrastructure Protection” (European Union Commission, December 12, 2006).

199 “Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, Decision No. 1106” (Organization for Security and Co-operation in Europe (OSCE), 2013); “Protecting Critical Energy Infrastructure from Terrorist Attack, Decision No. 6/07” (Organization for Security and Co-operation in Europe (OSCE), 2007); “Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace” (Organization for Security and Co-operation in Europe (OSCE), 2013).

supports elections and plebiscites.²⁰⁰ Nothing reflects genuine political sovereignty more than national participatory processes, such as elections. While the UN Charter sought to grant strong protections against undue external interference, those protective measures are challenged in the digital age. Voting system instruments and software may be vulnerable to attacks, while voter registration data is collected on a vast scale and published online.²⁰¹ Elections and participatory processes should be carried out in accordance with national laws, but cyber operations originating from outside a state's jurisdiction may necessitate a coordinated response. Norms such as these build upon and reaffirm international legal protections already afforded against external interference in the internal affairs of states, while calling for a commitment from governments as a modest first step toward effective multilateral cooperation. The success of the relevant norm put forward by the GCSC as well as a number of regional initiatives and national laws are evidence of general positive trends in the development of norms and rules in cyberspace.

3.2.4 Non-state actors should not engage in offensive cyber operations

The only norm that clearly shows a negative development is the case of 'hack-backs' or offensive cyber operations conducted by non-state actors. These non-state actors often justify their actions in the name of "self-defense," claiming that governments do not have the means to adequately protect them against cyber threats.²⁰² Because of the significant disruptive and damaging effects hack-backs might have, also for third parties, it may trigger complex international legal disputes and escalations. Yet, hack-backs are becoming more prevalent in practice, while widespread adoption of norms and rules prohibiting private-sector hack-backs is lacking. In some states, legislative initiatives to legalize hack-backs are circulated.²⁰³ Only recently have several proposals sought to

200 "Call to Protect the Electoral Infrastructure" (The Global Commission on the Stability of Cyberspace (GCSC), 2018).

201 "Call to Protect the Electoral Infrastructure."

202 Offensive cyber operations by non-state actors – or active cyber defense, as it has more commonly become known – should be understood as a set of measures ranging from self-defense on the victim's network to destructive activity on the attacker's network. Offensive operations within this continuum imply that the defender will act outside of its own network independently of its intention (offense or defense) and the legal qualification of its acts. For a discussion on offensive cyber operations, including the contextual and legal reasoning behind the capacity of states to take measures to protect non-state actors, see Global Commission on the Stability of Cyberspace, "Norm against Offensive Cyber Operations by Non-State Actors," in *Norm Package Singapore*, 2018.

203 See for example the Active Cyber Defense Certainty Act introduced in the US House of Representatives in 2017 that would allow private sector hack back. Tom Graves, "Active Cyber Defense Certainty Act," Pub. L. No. H.R. 3270 (2019).

curtail hack-backs – most notably the GCSC norm against offensive cyber operations by non-state actors,²⁰⁴ and the Paris Call on Trust and Security in Cyberspace.²⁰⁵

Overall, the development of regimes encompassing norms and rules in cyberspace is early work in progress. The functioning of these regimes requires multi-stakeholder engagement and compliance. While our analysis showcases the development of various important norms in this field, which are adopted by a growing number of states, diverging views especially between the East (Russia, China) and the West (Europe, the US) pose a significant challenge to the further development of the regimes in this sphere. In order to move on from norm development to first adoption and then compliance, stakeholders need to stand behind the norms both in words and in actions. Only once viable pathways for carrying those norms forward are identified will it become possible to assess norm adherence.

3.3 Hybrid Conflict

Hybrid conflict poses a significant challenge to the international order because ‘hybrid’ actors deliberately seek to circumvent the constraints imposed on them by existing international law. This section examines four norms and their sometimes explicitly formulated rules regulating hybrid conflict activities, concerning the use of proxy actors and states’ responsibility for these proxy actors, political interference, economic coercion, and disinformation campaigns. Unsurprisingly, given the nature and salience of hybrid conflict strategies in today’s strategic environment, our analysis paints a disconcerting picture. Unlike the cyberspace section, which looked at norm development, this section considers actual compliance.

204 Global Commission on the Stability of Cyberspace, “Norm against Offensive Cyber Operations by Non-State Actors.”

205 Ministry for Europe and Foreign Affairs of France, “Paris Call for Trust and Security in Cyberspace,” November 12, 2018.

Table 10 Hybrid conflict, multi-year regime estimate (up to 2025)

Norms	Trend
Norm of state accountability for their non-state actor partners	▼
Norm of non-interference in other states' election processes	▼
Norm of open, non-discriminatory trade between states	▼
Norm of non-interference in other states' societal discourse	▼

Rules	Trend
States are responsible for the conduct of the proxy actors they control (Article 8, Responsibility os States for Internationally Wrongfull Acts, 2001)	▼
States should not interfere with the internal affairs of another state, including publicizing the outcome of espionage campaigns to influence an election and targeting critical electoral infrastructure	▼
States cannot normally discriminate between their trading partners (Article 1, GATT 1994)	▼
States should not interfere with the internal affairs of another state, including the use of false propaganda to influence foreign electoral processes or create civil disarray	▼

■ Decreasing threat	■ Increasing threat	
▲ Upward	▼ Downward	▬ Net-zero / Stable

3.3.1 Norm of state accountability for non-state proxies

States have been increasingly relying on proxy actors to do their bidding, within but also outside of armed conflicts around the world. States are accountable for their non-state actor partners according to customary international law, amongst others. Article 8 of the International Law Commission's (ILC) Articles on the Responsibility of States for Internationally Wrongful Acts (2001) states that "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."²⁰⁶ It follows from this that states should be held responsible for the actions of their proxy actors, for instance when they violate international humanitarian law. This responsibility applies to actions both in the physical world and in cyberspace.²⁰⁷ The high threshold for determining what constitutes 'control', however, means that state responsibility is seldom established in practice.²⁰⁸ States are therefore seldom held to account. At the same time, actions conducted by proxy actors may trigger military and diplomatic repercussions outside the realm of international legal responsibility.²⁰⁹ With the greater prevalence of hybrid strategies and resulting heightened ambiguity, our assessment is that the norm of state accountability faces erosion.

3.3.2 Norm of non-interference in other states' election processes

While there is no explicitly codified norm in international law on non-interference in other states' election processes, core principles of international law appear to prohibit such interference. Reference can be made to the principle of non-intervention and the notion of national sovereignty, as enshrined in the UN Charter, under Articles 2(4) and 2(7). These involve not only sovereignty and territorial integrity, but also the conduct of foreign affairs and the choice of internal governance system. It can therefore be argued

206 It is important to note that the ILC Articles stem from customary international law. It took nearly 45 years and more than thirty reports by the ILC to come to an agreement, despite the general (and arguably vague) nature of the ILC Articles. Though these articles have not been enshrined in a binding treaty under international law, they constitute part of the wider binding framework of customary international law, given that the ICJ has referred to them and states have widely accepted the norms that these Articles represent. "Responsibility of States for Internationally Wrongful Acts" (2001).

207 Michael N. Schmitt and Liis Vihul, "Proxy Wars in Cyber Space: The Evolving International Law of Attribution," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, May 31, 2014).

208 Elena-Laura Álvarez Ortega, "The Attribution of International Responsibility to a State for Conduct of Private Individuals within the Territory of Another State (La Atribución De Responsabilidad Internacional a Un Estado Por La Conducta De Particulares En El Territorio De Otro Estado)," SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, January 1, 2015), 7–36.; for a detailed description of the tenets of 'strict control' and 'effective control' see pages 7–12 of the publication.

209 Schmitt and Vihul, "Proxy Wars in Cyber Space," 55–73.

that these principles also encompass the protection of critical electoral infrastructure.²¹⁰ States should refrain from interfering in another state's internal affairs. That includes campaigns to influence elections and the targeting of critical electoral infrastructure.²¹¹ Our assessment, however, is that external electoral interference has become more common in recent years. There have been instances of electoral interference in the US, in Western Europe, and in other regions around the world.²¹² While new international norms are being developed (see Table 10), the normative and regulative framework is facing erosion.²¹³

3.3.3 Norm of non-interference in other states' societal discourse

The use of propaganda and disinformation is regulated through various instruments, but most of these relate to conduct in war or to civil rights in domestic contexts.²¹⁴ However, the principle of non-intervention, as discussed in the previous section, is at odds with such behavior.²¹⁵ More recently, the Tallinn Manual specifically forbids the cyber-enabled manipulation of public opinion in elections, the alteration of online news services for the benefit of a particular political party, the spreading of false news, and

210 Nicholas Tsagourias, "Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace," *EJIL: Talk!* (blog), accessed December 11, 2019.

211 Please note that states relying on political espionage is a normal and well-established practice, but using the collected intelligence to undermine and interfere with foreign elections is in violation of the spirit of the norm of non-intervention. See Danny Pronk, "The Return of Political Warfare | Strategic Monitor 2018-2019" (Clingendael, 2018).

212 Jones and Taussig, "Democracy & Disorder: The Struggle for Influence in the New Geopolitics."

213 William Mattessich, "Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage," *Columbia Journal of Transnational Law*, August 15, 2016.

214 See for instance Article 20(1) of the International Covenant on Civil and Political Rights, which prohibits propaganda for war, or the Law of Armed Conflict (LOAC), which prohibits acts of perfidy – whereby perfidy is defined as "a deceptive practice intended to gain the opposition's confidence by assuring protection, and subsequently carrying out an attack as a breach of trust. Instances of perfidies include incorrect usages of white flags, symbols, uniforms and feigning cease-fires, amongst other things, and they are prohibited under LOAC." Unnati Ghia, "International Humanitarian Law In a Post-Truth World," *Cambridge International Law Journal* (blog), December 2018.

215 This is corroborated by international jurisprudence, including the judgment of the ICJ in the US-Nicaragua Case of 1986. The statement highlights how the principle of non-intervention extends from the political domain (discussed earlier in reference to political meddling) to the economic and civil domains. In this case, the Court re-affirmed that the principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States and that "a prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system..." "Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua vs. United States of America)," June 1986, 108.

the sabotage of a political party's online services.²¹⁶ While the overall norm of non-interference still exists, the greater prevalence and impact of disinformation campaigns shows that the norm is under pressure.

3.3.4 Norm of open, non-discriminatory trade between states

The norm of open, non-discriminatory trade is under threat, as will be discussed in greater depth in the section on free trade below. States are increasingly resorting to coercive economic measures to achieve their strategic objectives through targeted influence, and the exploitation of vulnerabilities and interdependencies.²¹⁷ This is taking place despite the existence of a well-developed international trade regime that prohibits the use of discriminatory trade practices under normal circumstances in the World Trade Organization (WTO) and its precursor, the General Agreement on Tariffs and Trade (GATT).²¹⁸ The violation of the principle of non-discrimination thus signifies a departure from the rules-based international liberal trading order. This is not to say that this trade regime is defunct, because for the most part states continue to adhere to the principle. Nevertheless, it does show that the norm of open, non-discriminatory trade has been negatively affected by the employment of economically coercive measures by states.

Overall, while recognizing that hybrid activities are designed to evade international law and avoid repercussions, our analysis corroborates the conclusion that the norms and rules that are part of the international regulatory framework relevant to hybrid conflict activities are under increasing pressure.

3.4 Economic Security

In the absence of global leadership, with the US apparently (and increasingly) losing in terms of relative power, the global norms and standards related to economic security are currently under pressure. This section discusses the most relevant developments that are affecting the international economic order and its functioning, in particular with reference to the free trade regime.

216 Nicholas Schmitt, "Rule 10—Prohibition of Threat or Use of Force," in *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013.

217 Muncher Sicherheitskonferenz, 'Munich Security Report 2019'.

218 Frieden, Jeffrey and Joel Trachtman, 'U.S. Trade Policy: Going It Alone vs. Abiding by the WTO'. Harvard University and the Fletcher School of Law and Diplomacy 2019.

Table 11 Economic security, multi-year regime estimate (up to 2025)

Norms	Trend
States are bound by a system of rules dedicated to open, fair and undistorted competition	▼
States resolve trade disputes within the multilateral framework of the WTO	▼
States refrain from taking protectionist measures	▼
(Trade) espionage is acceptable state behaviour when used for traditional purposes	▼

Rules	Trend
The broad regime of WTO rules and agreements on trade, goods and intellectual property rights	▼
Rules of non-discrimination (most-favoured-nation principle and national treatment)	▼

■ Decreasing threat	■ Increasing threat	
▲ Upward	▼ Downward	▬ Net-zero / Stable

3.4.1 A system of rules dedicated to open, fair, and undistorted competition

In addition to the potential economic effects of China’s BRI in European countries, such as potential debt traps, the BRI is also causing political discord within the EU. Thus, the BRI has been described as a deliberate tactic by Beijing to undermine EU unity. Even though major European countries are increasingly vocal in reaction to China’s unfair trade policies, investments, and unfulfilled reform promises, deals with the Chinese are still being signed (see chapter 2.4.2). The issue is dividing the EU. EU member states such as Germany and France have pushed for tougher screening criteria for Chinese investments, while other countries such as Greece and Portugal have adopted a more lenient approach.²¹⁹ There is growing concern about foreign investors, notably state-owned enterprises, that take over European companies for

219 Lucy Hornby et al., “Italy Set to Formally Endorse China’s Belt and Road Initiative,” *Financial Times*, March 6, 2019; Shi Jiangtao, “China, France Sign US\$45 Billion of Deals Including Airbus Order,” *South China Morning Post*, March 26, 2019; Alexandra Ma, “This Is China’s Playbook to Pit EU Countries against Each Other,” *Business Insider*, March 24, 2019; Jonathan E. Hillman, “Corruption Flows Along China’s Belt and Road,” *CSIS* (blog), January 18, 2019.

strategic reasons. In light of this, the EU has adopted a new framework for screening FDI into the EU, which came into force in April 2019.²²⁰ It provides a means of detecting and addressing security risks that may be posed by foreign takeovers of critical assets, technologies, and infrastructures. France and Germany are leading the push for a common strategy to deal with competition from Chinese state-led firms. In March 2019, the European Commission presented a new strategic ten-point action plan, marking a new approach in which the EU is openly moving to protect itself better in its trade relations with China.²²¹

Another development is that China has become a standard-bearer in the field of technology. The resulting risk is that some fields, such as IT, may splinter into US and Chinese spheres of influence. The strategic rivalry between China and the US is rapidly evolving into an arms race for technological dominance. China is highly proactive in influencing global tech standards (from AI to hydropower) and exporting its own standards along the 'Digital Silk Road'. European economies may find themselves increasingly dependent not just on US but also on Chinese digital technologies. This might also affect military operators, as they are increasingly dependent on technologies from the commercial sector (dual-use technologies). Also, Chinese companies are intensifying their influence in international standard-setting bodies. State-sponsored efforts to shape international standards have been ongoing since the country entered the WTO. A report by the UN World Intellectual Property Organization (WIPO) showed that China and the US are leading the global competition to dominate AI. Political trends in both countries imply that a growing divergence in IT systems and standards is likely.²²²

3.4.2 Settlement of trade disputes within the framework of the WTO

Probably the most evident example of increasing tensions in the international economic system is the chronic crisis surrounding the World Trade Organization (WTO). The US, under President Trump, is blocking the appointment of new members of the WTO Appellate Body, the organization's dispute settlement mechanism, thereby risking an existential crisis. On December 10, 2019, the Appellate Body became a lame duck,

220 "EU Foreign Investment Screening Regulation Enters into Force," Trade - European Commission, April 2019.

221 Lisbeth Kirk, "Europe Shifts Gear to Balance Relations with China Better," *EUobserver*, March 13, 2019; Jakob Hanke and Jacopo Barigazzi, "EU Accelerates Moves to Block China's Market Access," *POLITICO*, March 18, 2019; "EU-China Strategic Outlook: Commission and HR/VP Contribution to the European Council," Text, European Commission - European Commission, March 21, 2019; Keegan Elmer, "Europe's China Problem Is on the Agenda at next European Commission Meeting," *South China Morning Post*, February 27, 2019.

222 "EIU Global Forecast - Geopolitics Threatens Global ICT Order," The Economist Intelligence Unit, February 13, 2019; "WIPO Technology Trends 2019 - Artificial Intelligence," 2019; Rebecca Arcesati, "Chinese Tech Standards Put the Screws on European Companies," Mercator Institute for China Studies, January 2019.

with only one active judge out of the required three. This effectively paralyzes WTO enforcement at a time of heightened global trade tensions. Some argue that without effective dispute resolution there is a risk that the WTO system will collapse. Meanwhile, states are turning toward plurilateralism. A telling example is the recent announcement by 76 member countries that they will start independent negotiations on e-commerce, because in their opinion the WTO lacks vigor. All this highlights the increasing pressure on the norms and rules within the framework of the WTO, and thus the need for reforms within the organization.²²³

Overall, it can be concluded that China is taking a prominent place with regard to several developments in the international order, including the evolving trade war between the US and China, standards-setting within the field of technology, and the expansion of the BRI in European countries. Hence, economic security and prosperity will increasingly be dependent on Chinese economic policies, and more broadly on China's stance toward and its activities in the international order.

3.5 CBRN Weapons

The increasing pressure on the international order can also be observed in the field of CBRN weapons. In particular, this concerns pressure on the existing CBRN arms control treaties. Hence, the first important development identified in our horizon scan refers to the demise of existing CBRN arms control treaties.

223 Alice Poidevin, "What Does the Future Hold for US Trade Policy?," *European Centre for International Political Economy* (blog), February 2019; "Splintergroep Binnen WTO Gaat Werken Aan Regels Voor E-Commerce," *Financieel Dagblad*, January 2019; Iryna Bogdanova, "WTO Dispute on the US Human Rights Sanctions Is Looming on the Horizon," *EJIL: Talk!* (blog), January 2019.

Table 12 CBRN weapons, multi-year regime estimate (up to 2025)

Norms	Trend
States should work towards a world without CBRN weapons	▼
CBRN weapons should never be used	▼

Rules	Trend
States should work towards a world without CBRN weapons	▼
Arms control agreements should not be violated	▼
Access of non-state actors to CBRN weapon materials should actively be prevented	—

▲ Upward ▼ Downward — Net-zero / Stable

3.5.1 A world without CBRN weapons

Several experts are worried about the nuclear programs of Saudi Arabia and Iran. In the case of Saudi Arabia, experts are concerned that the civilian nuclear program might be a stepping stone toward the actual development of nuclear weapons. Experts assume that Saudi Arabia would want to develop these weapons in order to match the capacities of Iran. Concerns about Iran’s nuclear program pertain to the disintegration of the Joint Comprehensive Plan of Action (JCPOA). Iran has so far refrained from taking serious steps toward the direct development of nuclear weapons, but, since the withdrawal of the US, the country has diverged from the limits set under the JCPOA. If the problems around the JCPOA are not resolved, it is not impossible that Iran might take more serious action. Hence it can be said that states are decreasingly focused on working toward a world without CBRN weapons.

3.5.2 The use of CBRN weapons

A second worrisome development is the fact that the threshold for the use of nuclear weapons is lowering. This can be seen in the changing political rhetoric on nuclear weapons, including implicit threats of using nuclear weapons and the perception that the use of nuclear weapons is an actual option available to states. Russia has warned

of a crisis like the Cuba crisis of 1962 in response to possible NATO actions after the demise of the INF treaty. Likewise, the fact that the US Nuclear Posture Review 2018 allows for the use of nuclear weapons in response to non-nuclear threats signals the idea that nuclear weapons can legitimately be used, even if a state is not attacked first with nuclear weapons.²²⁴ This severely violates the established and widely accepted international norms and rules that CBRN weapons should never be used. In addition, when states regard the use of nuclear weapons as legitimate, they indirectly violate the NPT, as they are not working toward a world without CBRN weapons.

3.5.3 Prevention of increased access of non-state actors to CBRN weapons

The proliferation of CBRN technology is not limited to states. Developments in science and technology and the diffusion of knowledge make the access, use, and proliferation of CBRN technologies easier for non-state actors. This applies particularly to advances in the biological and chemical fields.²²⁵ Hence, efforts to prevent access of non-state actors to CBRN materials should intensify.

3.5.4 Arms control agreements are under pressure

For several years, the United States and Russia have been accusing each other of violating the INF treaty. The accusations eventually culminated in the withdrawal of both parties from the treaty, leaving Europe exposed to potential renewed deployment of intermediate range ballistic and cruise missiles on Russian soil. As described in the section on military competition, the demise of the INF treaty seems to be a symptom of a wider trend, in which political actors are questioning and criticizing current arms control agreements. For example, in anticipation of the expiration of New START in 2021, important actors in the US government and military have expressed doubts about the chances that New START will be continued and are questioning whether the treaty even should be. They cite Russian violations of the INF treaty and the fact that various arms control treaties do not include states like China.

224 Maria Kiselyova, "Russia Warns of Repeat of 1962 Cuban Missile Crisis," *Reuters*, June 24, 2019.

225 Névine Schepers, "Q&A: Understanding Saudi Arabia's Nuclear Energy Programme," *IJSS* (blog), April 30, 2019; Aileen Murphy, "The Trump Administration Is Eager to Sell Nuclear Reactors to Saudi Arabia. But Why?," *Bulletin of the Atomic Scientists* (blog), April 16, 2019; Brockmann, K, Bauer, S, and Boulanin, V, "Arms Control and the Convergence of Biology and Emerging Technologies"; Daryl Kimball, "The Trump Administration's Failing Iran Policy Is Spurring Troubling Retaliatory Actions by Iran," Arms Control Association, accessed December 20, 2019.

In addition, the withdrawal of the US from the 'Iran Deal', or JCPOA, has put the entire deal under extreme pressure. The US' approach to Iran seems more focused on regime change than on restricting Iran's nuclear program, leading to increased tensions in the region and increased risk of the deal falling apart completely.

Other cornerstones of the CBRN arms control architecture are under pressure as well. Many states are disappointed in the NPT because they consider that the disarmament efforts of the treaty have not been fulfilled. Furthermore, the cases of chemical weapons being used in the United Kingdom, Malaysia, and Syria in the past few years are serious violations of the Chemical Weapons Convention. Experiments with lethal viruses appear to violate the Biological Convention and, last but not least, there are accusations (without convincing evidence so far) that Russia has been testing low-yield nuclear weapons in violation of the Comprehensive Test Ban Treaty (CTBT).²²⁶ These examples demonstrate that the international arms control regime is under severe pressure, leading to potential questioning of its effectiveness. Trust issues regarding the multilateral system for CBRN weapons are therefore emerging.

3.5.5 Violations of existing arms control agreements

Lastly, a persistent problem is the lack of an effective sanctions regime that condemns the use of CBRN weapons. In particular, the perceived impunity of the use of chemical weapons bears the risk of undermining the global norm against chemical weapons set by the Chemical Weapons Convention. The chemical weapons used in Syria, Malaysia, and the UK show that actors, both state and non-state, are not refraining from using this type of weapon. This is closely related to the fact that, so far, the perpetrators have faced few serious consequences. This perceived impunity may encourage other actors to use chemical weapons as well.²²⁷

226 "For Decades, the United States and Russia Stepped Back From the Brink. Until Now," *The New York Times*, February 10, 2019, sec. Opinion; Douglas Barrie, "Ground-Launched Cruise Missiles, Europe and the End of the INF Treaty?," *IISS* (blog), February 2019; Daryl G. Kimball, "Bolton's Attempt to Sabotage New START | Arms Control Association," Arms Control Association, August 2019; Ashley Roque, "USSTRATCOM Commander Paints Dour Future for New START," *Jane's 360* (blog), February 2019; Robert Einhorn and Richard Nephew, "Constraining Iran's Future Nuclear Capabilities," *Brookings* (blog), March 26, 2019; Graeme Wood, "How Long Can John Bolton Take This?," *The Atlantic*, July 2, 2019; Fei Su and Ian Anthony, "Reassessing CBRN Threats in a Changing Global Environment"; Mark Urban, "Salisbury 'shows' Russia Stockpiling Weapons," *BBC News*, March 4, 2019, sec. UK; Steven Andreasen, "Trump Is Quietly Leading Us Closer to Nuclear Disaster," *Washington Post*, June 2019.

227 Fei Su and Ian Anthony, "Reassessing CBRN Threats in a Changing Global Environment"; Alicia Sanders-Zakre and Daryl Kimball, "Responses to Violations of the Norm Against Chemical Weapons," *Arms Control Association* (blog), April 2019.

Overall, it can be concluded that the international non-proliferation framework is now under severe pressure, fueling serious concerns about the future of arms control itself. For the Dutch, being traditional stalwarts of the international legal order, this will be of immediate impact, not only from an international judicial perspective, but – and increasingly so – also from a national security perspective.

3.6 Terrorism

New and emerging technologies offer new opportunities, not only for terrorists but also for those fighting them. Thus, in contrast to the fields discussed above, our assessment regarding the international order in the field of counterterrorism is more favorable. Overall, most of the trends identified show a decreasing movement, whereby, for instance, both state and non-state actors are drafting new norms and rules, but also complying with the existing rules and norms. Underscoring this development is the December 2019 reduction of the threat level in the Netherlands, from level 4 to 3 (on a 1–5 scale).²²⁸

228 Rijksoverheid, “NCTV: Dreigingsniveau Naar 3, Aanslag in Nederland Voorstelbaar,” December 2019.

Table 13 Terrorism and technology, multi-year regime estimate (up to 2025)

Norms	Trend
The use of AI by state and non-state actors should be based on ethical standards	—
Big tech companies should be co-responsible for removing terrorist content from their platforms	▲
Trade and transfer of lethal drone technology should be regulated by legally binding standards	▲
Private companies should be involved in developing and setting ethical frameworks for the governance of AI	▲

Rules	Trend
Initiatives by state- and non-state actors to set ethical standards regarding the use of AI	▲
The number of legal measures that increase tech companies' responsibility to remove terrorist content	▲
Initiatives by state and non-state actors to regulate the trade and transfer of lethal drone technology by legal standards	▲
The development of private-public partnerships working towards establishing ethical guidelines for the use of AI	▲

■ Decreasing threat	■ Increasing threat	
▲ Upward	▼ Downward	— Net-zero / Stable

3.6.1 The protection of ethical standards in the use of AI

The ongoing development in AI poses new security challenges, but also opens up an array of possibilities, for example in the field of counterterrorism. With the support of private companies, states are increasingly deploying – or looking into deploying – AI-based predictive software combined with Big Data analytics, aimed at surveillance, tracking, processing, identification, and ultimately disruption of potential terrorist behavior. Existing AI-based analytical applications are constantly being improved and refined. AI is also central to the newest moderation software deployed by tech companies aiming to rid their social media platforms of extremist content.²²⁹

These new technologies have significantly enhanced states' ability to counter terrorism and are expected to play an even more central role in our counterterrorism efforts. However, the use of new technologies such as facial recognition is putting pressure on human rights, both intentionally and unintentionally. The use of AI solutions may threaten freedom of expression, impact citizens' right to privacy, drive inequality and discrimination, and provide repressive regimes with powerful tools to control their populations. These dilemmas are fueling intense policy debates on legislation, binding norms, and the governance of AI.²³⁰

3.6.2 Responsibility of private companies

With respect to the role of private (tech) companies in this field, despite positive developments that can already be observed, there is room for improvement. Big tech companies are willing to make an effort but are reluctant to accept legal accountability for the removal of extremist content. In fact, big tech companies are extensively supporting lobbying efforts in attempts to influence or block potential regulation that would attribute responsibility for illegal content to them, in spite of public statements that they are open to government oversight.²³¹

229 Errol van Engelen, "Big Data Will Effectively Fight Terrorism In The World," *Datafloq*, January 2019; "UNOCT Consolidated Multi-Year Appeal 2019-2020" (UNOCT, 2018).

230 Kathleen McKendrick, "Artificial Intelligence Prediction and Counterterrorism" (Chatham House, August 2019); Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *The New York Times*, April 14, 2019, sec. Technology; Ni Aolian, "European Counter-Terrorism Approaches: A Slow and Insidious Erosion of Fundamental Rights," *Just Security*, October 17, 2018; Ben Wagner et al., "Surveillance and Censorship: The Impact of Technologies on Human Rights" (European Parliament), accessed December 6, 2019; "Artificial Intelligence: Expert Committee to Explore the Development of a Legal Framework," September 2019.

231 David Ibsen, "Big Tech Spends Millions to Shape Possible Regulation of Extremist Content Online," *Counter Extremism Project* (blog), May 8, 2019; Alexandra S. Levine, "Facebook, Twitter and Google Testify on Extremism," *POLITICO*, September 18, 2019; Martyn Frampton, Ali Fisher, and Nico Prucha, "The New Netwar: Countering Extremism Online," *Policy Exchange* (blog), September 23, 2017.

3.6.3 Private-public partnerships working toward ethical guidelines

A positive development in the field of terrorism and technology is the increasing level of cross-platform and cross-industry collaboration. The Christchurch attack of March 2019 has prompted tech companies, backed by governments, to launch the Christchurch Call to Action. This initiative focuses on cooperation and the sharing of best practices among tech industry rivals, across platforms and among nations to improve digital fingerprinting technologies, develop better oversight of post-attack live streaming, more effective moderating tools, and algorithms to promote redirection to counter narratives. With increasingly institutionalized initiatives such as the Global Internet Forum to Counter Terrorism, big tech companies are becoming ever more independent players in the fight against terrorism and online radicalization, while at the same time actively searching collaboration opportunities with governments and academia.²³²

In a similar vein, realizing the cross-border nature of terrorist threats, international organizations like the EU and the UN are increasingly aware of the importance of easy access to crucial information on terrorist activity, movements, convictions, prosecutions, and investigations. For that purpose, these organizations are launching new and optimizing existing technical tools. Databases such as the Counter Terrorism Register and software such as Go Travel enable law enforcement agencies to easily access and share intelligence. The efficacy of sharing data across jurisdictions is still limited by privacy laws, and concerns remain about abuse of these data sharing and collaboration efforts by illiberal regimes.²³³

3.7 Sub-conclusions

The trends and developments in the international order present a negative picture with regard to the four themes of military competition, hybrid conflict, economic security, and CBRN weapons. For all four themes, the degree of cooperation in the international order is shifting toward increased contestation of the norms and rules of existing regimes. Trends and developments related to norm development in cyberspace and norm compliance on the terrorism-technology nexus are decidedly more positive. Here,

232 Joshua A. Geltzer, Karen Kornbluh, and Nicholas Rasmussen, "Tech Companies Must Fight White Supremacy, Regardless of Political Dangers," *Lawfare*, August 7, 2019; Patrick Tucker, "Big Tech Bulks Up Its Anti-Extremism Group. But Will It Do More than Talk?," *Defense One*, September 2019; Amrita Khalid, "Anti-Extremism Group Run by Social Media Giants Becomes Independent," *Engadget*, September 23, 2019.

233 "UN Launches Innovative Programme to Detect and Disrupt Terrorist Travel," *UN News*, May 7, 2019; "INTERPOL and UN Publish Joint Handbook for Online Counter-Terrorism Investigations," *Interpol*, July 2019; "Terrorism Evolving: Insights from Research to Combat the Threat," *Europol*, April 2019.

we see the development of new norms in cyberspace and cooperation in international counterterrorism efforts. Our analysis warrants the following sub-conclusions.

First, our analysis finds that both norms and rules regulating various forms of military competition are facing significant erosion. The international regulatory framework has been facing considerable problems with a lack or reversal of progress in areas pertaining to nuclear and conventional arms control, and reduced state adherence to the norms and the rules upon which it rests.

International regulatory attempts to constrain states' cyberspace activities have had some success, even though considerable divergence is emerging in multilateral fora on how international rules should be interpreted. While the ability of states to regulate this domain is hindered by rapid technological developments, an unwillingness to regulate e-tech companies for fear of hindering innovation, difficulties in attribution, and the important role of non-state actors, a number of core initiatives in the field of norm development have been taking root over the last couple of years. Within this multi-stakeholder setting, our analysis of the development of norms, rather than compliance with norms, paints a more positive picture than for the other domains.

In the hybrid domain, where compliance with norms was assessed, that picture is much more negative. Acknowledging that hybrid conflict activities are typically aimed at circumventing existing international law, our analysis supports the conclusion that states increasingly infringe upon existing international regulatory regimes relevant to hybrid conflict activities.

In the economic sphere, states' policies are undermining the norms of a system dedicated to open, fair, and undistorted competition while they fail to live up to salient rules and regulations. Examples include the increasing number of protectionist policies adopted by states and the consistent weakening of the WTO as the salient organization to settle trade disputes.

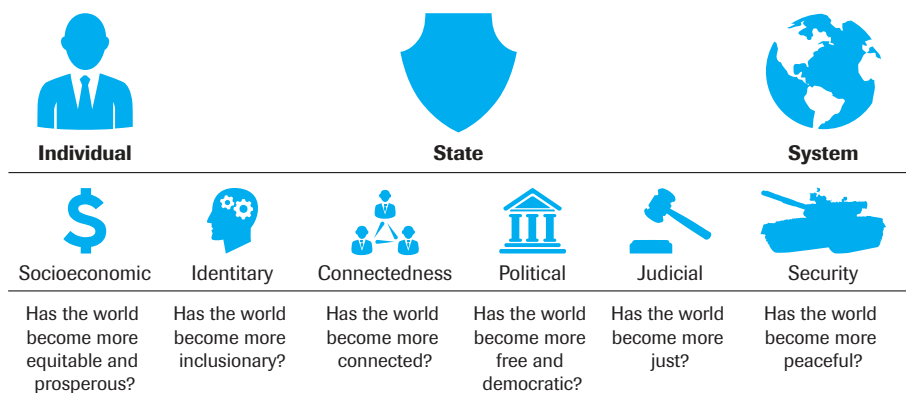
With reference to CBRN weapons, states increasingly appear to ignore long-established and agreed-upon norms and rules that CBRN weapons should never be used, and moreover fail to work collectively toward a world without CBRN weapons.

Finally, the field of counterterrorism features a variety of promising trends involving greater cooperation between states and non-state, private actors in regulating the access to and use of new and emerging technologies.

4 Geodynamics

To capture dynamics in a world that is in a state of flux, this chapter looks at trends and developments at multiple levels across different domains. Previous iterations of the Strategic Monitor introduced the term ‘geodynamics’ to capture a broader spectrum of trends and developments at multiple levels.²³⁴ The ‘geo-’ in geodynamics stands for the Greek word γῆ (gê), or Earth. Geodynamics takes a multi-perspective approach and analyzes dynamics at the level of the international system, of the state, and of individuals; and across the socio-economic, identity, connectedness, judicial, political, and security domains (see Figure 1).²³⁵

Figure 1 Geodynamics: six domains, three levels



²³⁴ The term geodynamics was first introduced and further conceptualized in 2016 in the Report *The Wheel of Fortune*, pp. 91-110, with assessments in the contributions to the Dutch government’s Strategic Monitor. See Stephan De Spiegeleire, Khrystyna Holynska, and Yevhen Sapolovych, “Things May Not Be as They Seem: Geo-Dynamic Trends in the International System,” 2018; Stephan de Spiegeleire et al., “Nowcasting Geodynamics, Great Powers and Pivoting” (The Hague: The Hague Centre for Strategic Studies, 2017); Stephan De Spiegeleire et al., “Stilte Voor de Storm?,” 2018.

²³⁵ Steven Pinker, *Enlightenment Now: The Case for Reason, Science, Humanism, and Progress*, 1st Edition (New York, New York: Viking, 2018); Julian L. Simon, *The State of Humanity*.




For each domain and each level, the central question is assessed on the basis of two indicators: whenever possible, one of these indicators is objective in nature and examines the actual state (of equality, freedom, security), while the other is subjective in nature and examines how this state is experienced or perceived by individuals. This makes for a total of 36 indicators for which data has been collected, collated, and combined from academic, NGO, and public institution data sources.²³⁶ Where possible, the period of measurement stretches from the beginning of this century to the most recent data point available. Progress is measured over the whole period and for the last two years for which there was data available.

A note of caution is in order for the interpretation of the results. The six central questions posed in this chapter are open not only to interpretation but potentially also to ideology: notions such as 'freedom' and 'justice' are not without ideological baggage. They are also aggregated, combining a range of sub-themes and underlying indicators. As a result, indicators to measure important geodynamic developments with global coverage are not as commonly established and data are not as frequently collected and updated as in more established and focused disciplines. Therefore, in putting together this overview, we faced difficult choices in the selection of indicators to shed light on broader developments, and we are aware that other indicators with as much or potentially even more relevance or explaining power were left out. Also, especially for some of the subjective indicators, information is relatively outdated. If this was the case, we have sought to update, corroborate, and triangulate the observed trends based on complementary literature. The geodynamics approach and the measurements of associated indicators will continue to be developed as part of building up the strategic anticipation function in the context of the strategic monitor.

236 For a more elaborate description and explanation, see Hugo van Manen et al., "Methodological Annex: What World Do We Live In?" (Hague Centre for Strategic Studies, January 2020).

4.1 Socio-economic

Table 14 Has the world become more equitable and prosperous?

	Observation level	Indicator	All available dates	2 most recent years	Time range
	Subjective	Financial satisfaction	▲	▼	2000 - 2014
	Objective	Human development	▲	▲	2000 - 2017
	Subjective	Spending on healthcare and education	▲	▲	2000 - 2016
	Objective	Internal inequality	▲	▲	1980 - 2017
	Subjective	Perception that working hard gets one ahead	▲	▲	2007 - 2018
	Objective	International inequality	▼	▲	2000 - 2018

Developments in the socio-economic domain comprise a fair amount of positive but also some negative developments. Overall, human development remains decidedly positive. More than one billion people have been lifted out of extreme poverty since 1990.²³⁷ The Global Human Development Index has increased by about 27% since the 1990s.²³⁸ This has been accompanied by an increase in perceived financial satisfaction over the longer term, with some fluctuation in recent years. In the World Values Survey, people responded predominately positively to the question of whether they were satisfied with the financial situation of their household, although this trend has stagnated over the last two years. More people believe that working hard enables them to advance. At the global level, policy debates about the retrenching role of the state notwithstanding, governments have been investing a growing share of their annual budgets in social protection and human development.²³⁹ Following a slump after the 2008 Financial Crisis, there has been a marked increase in the degree to which governments invest in

237 "United Nations Millennium Development Goals," accessed November 20, 2019.

238 "Human Development Reports - 2018 Statistical Update," 2018.

239 Esteban Ortiz-Ospina and Max Roser, "Government Spending," *Our World in Data*, 2016.

healthcare and education, both of which are known drivers of human welfare.²⁴⁰ From 2000 to 2016, global spending on healthcare increased by an average 6% in low- and middle-income countries and 4% in high-income countries.²⁴¹

However, inequalities in income and wealth, which have been and continue to be hotly debated, have both increased according to various measurements, most importantly in measurements that look at the degree of wealth held by the 'one percent'.²⁴² The global average of national Gini (income inequality) coefficients saw a slight decrease in the last two decades based on traditional Gini assessments used by the World Bank and the IMF. However, various other measurements suggest that inequality has been increasing.²⁴³ According to data from Oxfam and the World Inequality Lab, measurements relating to both income and wealth inequality within states indicate a rise in inequality. In the share of income held by the wealthiest 10%, except for Russia, no region has recorded a very steep increase over the past decades. Small increases in income inequality nevertheless appear everywhere except in the Middle East and Brazil. Europe continues to be a relative beacon of equality.²⁴⁴

Interestingly, inequality between states as measured in GDP per capita has decreased, indicating a smaller gap between 'rich' and 'poor' states. At the same time, as borne out by the Gini coefficient, global inequality still stands at 0.64 out of 1 (with 1 being complete inequality: all resources are held by one actor), indicating that high levels of inequality at the system level persist.²⁴⁵ For comparison, the most non-egalitarian countries in the world, South Africa and Namibia, have lower Gini scores (0.63 and 0.59 respectively²⁴⁶) than the international level.

At the system level, global wealth is also lopsidedly distributed to a greater degree than before. In 2009, 380 billionaires held as much wealth as the poorest 50% of society that year – and by 2017 as few as 48 billionaires held this much. The world's wealthiest individuals, i.e., those holding over \$100,000 in assets, make up less than 10% of the world's population but possess 84% of global wealth. Individuals worth more than \$30 million, a group which represents a mere 0.003% of the world population, command

240 Xu Ke, Priyanka Saksena, and Alberto Holly, "The Determinants of Health Expenditure: A Country-Level Panel Data Analysis," *World Health Organisation*, 2011, 28.

241 Ke Xu et al., "Public Spending on Health: A Closer Look at Global Trends" (World Health Organisation, 2018).

242 "Economists Are Rethinking the Numbers on Inequality," *The Economist*, November 28, 2019.

243 See for example "Human Development Reports - 2018 Statistical Update"; Facundo Alvaredo et al., *World Inequality Report 2018* (Harvard University Press, 2018).

244 Alvaredo et al., *World Inequality Report 2018*, 20.

245 The World Bank Group, "GDP per Capita (Current US\$)," The World Bank Data, 2018.

246 "GINI Index (World Bank Estimate) - South Africa | Data," accessed November 26, 2019.

a staggering 11.3% of global wealth.²⁴⁷ This points to another trend which is not visible in traditional Gini income measures: the income share of the middle four deciles, particularly in the developed world, has fallen by two percentage points on average.²⁴⁸ This hollowing out of the middle class has important ramifications for developments in the identity, political, and judicial domains,²⁴⁹ fueling disenfranchisement and in-group, out-group dynamics.²⁵⁰

The overall answer to the central question of whether the world has become more prosperous and equitable is therefore paradoxical. Yes, the world has become more prosperous as a whole, and the world's poor have also seen significant improvements. But inequality within states has worsened due to a variety of measures, and while inequality between states has decreased, overall levels leave ample room for improvement.

247 "Global Inequality," Inequality.org, accessed November 21, 2019.




248 See Alvaredo et al., *World Inequality Report 2018*; Branko Milanovic, "Description of All the GINIS Dataset" (Stone Center on Socio-Economic Inequality, 2019). See also Branko Milanovic, "Description of All the GINIS Dataset" (Stone Center on Socio-Economic Inequality, 2019).

249 It is important to note that recent research suggests that – by some metrics – the middle class has not been "hollowed out" to the degree that was previously thought, though few argue that it has become *better off* over time. See "Economists Are Rethinking the Numbers on Inequality."

250 Nat O'Connor, "Three Connections between Rising Economic Inequality and the Rise of Populism," *Irish Studies in International Affairs* 28 (2017): 29–43.

4.2 Connectedness

Table 15 Has the world become more connected?

	Observation level	Indicator	All available dates	2 most recent years	Time range
	Subjective	Trust in peers	▼	▲	2005 - 2014
	Objective	Informational connectedness	▲	▼	2005 - 2014
	Subjective	Depth of diplomatic connections	▲	—	2000 - 2013
	Objective	Level of globalization	▲	▲	2000 - 2018
	Subjective	Number of diplomatic events	▼	▼	2000 - 2019
	Objective	Volume of international exchanges	▲	▼	2000 - 2016

Levels of connectedness between states, societies, and individuals are increasing according to various measurements. But these increases do not necessarily translate into increasing levels of interpersonal trust. The ICT revolution of the past twenty-five years is a principal driver behind increased connectedness. The share of the world population using the Internet continues to increase, with currently over half of the world population connected to the Internet.²⁵¹ The spread of the Internet marks a milestone in the history of social technologies. It has contributed not only to an exponential increase in the cross-border exchange of information, but also to the flow of goods and services as well as people. As such, it is a key enabler of a connected world, harnessing both promises and pitfalls.

Individuals have access to more – and more varied – sources of information, with the amount of information sources accessed on average nearly doubling between 2005 and 2014 according to the World Values Survey.²⁵² Informational connectedness is accelerating the spread of news and facilitating new forms of knowledge production and collaboration. At the same time, ICT also plays a part in dislodging individuals from their

251 Max Roser, Hannah Ritchie, and Esteban Ortiz-Ospina, “Internet,” *Our World in Data*, 2019.

252 Christian Welzel, “WVS 1 to 6 Key Aggregates, Version 1” (Lueneburg, Germany, 2014).

physical environment, substituting social embeddedness for virtual interactions in an online environment. These technologies thus reinforce the ‘bowling alone’ effect through their distorting effect on civic engagement and subsequently on the social fabrics that shape society.²⁵³ In addition, several trends point toward the development of information consumption in largely separated media ecosystems, facilitating the development of online ‘echo chambers’, which can contribute to ‘social bubbles’ structured around narrow preferences in norms and values, driving societal isolation and polarization.²⁵⁴ The news on this count is therefore mixed.

At the international and the system level, connectedness has increased since the beginning of this century. The KOF Globalization Index from the Swiss Economic Institute, which measures globalization along a wide range of economic, social, and political dimensions, records growth in globalization of just under 20% between 2000 and 2017. Alongside that development, states are investing more in their diplomatic reach worldwide, and diplomatic representation worldwide has increased. At the system level, the scope and size of interstate relations in the economic, political, security domain have also increased considerably according to the Formal Bilateral Influence Capacity Index (FBICI) of the Frederick S. Pardee Center for International Futures.²⁵⁵ State interactions, meanwhile, are paradoxically declining in relative terms, although we admit that the measurement is far from perfect.²⁵⁶ Our analysis based on GDELT data and corroborated by ICEWS data shows a decline in the number of international diplomatic events relative to the total number of international events of roughly 9%.²⁵⁷

Overall, these observations reflect an increase in diplomatic representations as well as in the degree of connectedness of the world at large. At the same time, stagnating or decreasing growth is present in the level of international exchanges, the pace of globalization, world diplomatic interactions, and individuals’ trust in their peers. Yes, the world has become more connected, although growth has been slowing, and it has not necessarily brought the world closer together.

253 Robert Putnam, *Bowling Alone: The Collapse and Revival of American Community* (New York: Simon & Schuster, 2000).

254 John D. Boy and Justus Uitermark, “Reassembling the City through Instagram,” *Transactions of the Institute of British Geographers* 42, no. 4 (2017): 612–624; Michela Del Vicario et al., “Echo Chambers: Emotional Contagion and Group Polarization on Facebook,” *Scientific Reports* 6, no. 1 (December 1, 2016): 1–12.




255 Jonathan D. Moyer et al., “Power and Influence in a Globalized World” (Washington, DC: Atlantic Council, Frederick S. Pardee Center for International Futures and HCSS, January 2018).

256 The GDELT dataset records prevalence of diplomatic events based on media reports. Therefore, a decreasing trend could also mean that diplomatic events receive (relatively) less attention in the media, while they still occur with the same frequency. The nature of the data makes it impossible to control for this possibility.

257 The GDELT Project, “The GDELT Project: Data,” 2019.

4.3 Identity

Table 16 Has the world become more inclusionary?

	Observation level	Indicator	All available dates	2 most recent years	Time range
	Subjective	Trust in out-groups	▼	▲	2005 - 2014
	Objective	Inclusiveness	▼	▼	2016 - 2018
	Subjective	Social hostilities	▲	▲	2007 - 2016
	Objective	Religious restrictions	▲	▲	2007 - 2016
	Subjective	Populist discourse	▲	▲	2000 - 2018
	Objective	Votership for populist parties	▲	▲	2000 - 2018

Trends within the identity domain are largely negative, with some exceptions. Trends in this domain reveal an increase in identity-driven politics in Western Europe, North America, and Latin America. Populist parties have received a larger share of the vote in national elections, while political leaders more frequently deploy populist rhetoric. The magnitude of populist discourse is captured in the Global Populism Database and ranges from 0 (not populist) to 2 (very populist). Since 2000, the average score for Western European populist discourse climbed most markedly from 0.18 to 0.45. Although soon to be overtaken by Western Europe, the world’s most populist region up until now was Latin America, with countries such as Venezuela and Bolivia ranking among the most populist governments in the world.²⁵⁸ Similarly, the average European populist vote has increased from 13.5% in 2000 to 24% in 2019.²⁵⁹ It reflects a broader trend in which in-group/out-group dynamics have become more prevalent in politics. This tendency is not limited to the Western world but is also prevalent in other parts of the world including South Asia (e.g., India) and South East Asia (e.g., the Philippines and Myanmar).

258 “Coding Rubric and Anchor Texts for the Global Populism Database” (The Guardian, March 5, 2019).

259 Timbro Authoritarian Populism Index, “The Data,” Timbro Authoritarian Populism Index 2019, February 2019.

At the state level, states have implemented a greater number of religious restrictions. Social hostilities involving religion have increased too. Our measurement relies on data from PEW Research Center, which only runs from 2007 to 2016 and reveals a negative trend for that period. The latest data indicates increases since then, showing that 52 governments impose “high” or “very high” levels of religious restrictions on their populations – a rise from forty countries in 2007.²⁶⁰ Alongside that trend, social hostilities involving religion reveal a more nuanced picture but are negative on balance. Substantial increases are reported in hostilities related to religious norms, with less marked increases in harassment by individuals and social groups and religious violence by organized groups.²⁶¹ While high in the Middle East over the entire period between 2007 and 2017, social hostilities related to religious norms have increased most sharply in North and South America, Sub-Saharan Africa, and Europe. Europe saw the steepest increase in religious social hostilities, mainly because key EU countries, such as Germany, France, or Italy, rank among the top increasers in terms of violence related to religious norms in 2017.²⁶²

At the individual level, both the level of inclusiveness and trust in out-groups have declined since the turn of the century.²⁶³ The Inclusiveness Index measures acceptance of out-groups and levels of discrimination in both official/institutional and unofficial contexts,²⁶⁴ taking into account race, gender, religion, and disability, and including an analysis of discriminatory laws, representation of minorities in parliament, the number of refugees a country has accepted, etc.²⁶⁵ Western countries continue to lead in overall inclusiveness. There are slight drops in inclusiveness in Europe and Asia. Latin America and the Caribbean have become more inclusive, albeit starting from lower baseline scores. Awareness of gender and racial inequalities, facilitated by social media and triggering increased social awareness and mobilization, has contributed to positive changes in several countries.²⁶⁶ The MeToo movement, for example, continues to galvanize international attention and is effecting real changes in norms regarding gender relations.²⁶⁷

260 Pew Research Center, “How Religious Restrictions Have Risen Around the World,” *Pew Research Center’s Religion & Public Life Project* (blog), July 15, 2019.

261 Pew Research Center.

262 Pew Research Center.

263 Note: The data indicates a small increase in trust in out-groups measurement between 2012-2014 (the two most recent years). However, due to the nature of the World Values Survey Data (sampling a different set of countries each year) year-to-year comparisons are not meaningful.

264 Haas Institute for a Fair and Inclusive Society, “2018 Inclusiveness Index,” December 2018.

265 Haas Institute for a Fair and Inclusive Society.

266 Laura Silver and Christine Huang, “Appendix A: How Smartphone and Social Media Use Relate to Social Network Diversity,” *Pew Research Center: Internet, Science & Tech* (blog), August 22, 2019.

267 “#MeToo Movement’s Second Anniversary,” Human Rights Watch, October 14, 2019; Human Rights Watch, “ILO: New Treaty to Protect Workers from Violence, Harassment,” Human Rights Watch, June 21, 2019.




Increased awareness of social issues has, however, not always translated into increases in inclusiveness in the wider society. In some cases, it coexists with decreases in out-group trust. At the individual level, trust in strangers decreased between 2005 and the latest available data from 2014. Evidence from the General Social Survey project tends to support the notion that individuals approach others with a fair amount of distrust. In 2018, only 21% of the people surveyed agreed that people can generally be trusted, as opposed to 42% who disagreed.²⁶⁸ Although the question of why trust in out-groups has declined is a complex one, it may be at least partially attributed to the social impacts associated with modernization and globalization.²⁶⁹ Overall, the answer to the question of whether the world has become more inclusionary boils down to a qualified no.

268 Tom W. Smith et al., “General Social Surveys, 1972-2018” (National Science Foundation, December 2019).

269 Simon Bornschieer and Hanspeter Kriesi, “The Populist Right, the Working Class, and the Changing Face of Class Politics,” 2013, 10–29.

4.4 Political

Table 17 Has the world become freer and more democratic?

	Observation level	Indicator	All available dates	2 most recent years	Time range
	Subjective	Desire to live in democracy	▼	▼	2005 - 2014
	Objective	Voter turnout	▼	▼	2000 - 2018
	Subjective	Perceived democracy	▼	▼	2005 - 2014
	Objective	Polity IV scores	▲	▲	2000 - 2018
	Subjective	UNGA voting disagreement	▼	—	2000 - 2018
	Objective	Number of people living under democracy	—	▲	2000 - 2018

In the last two decades, the world at large has become more democratic when measured in terms of the number of people living in democracies and the actual number of democracies, but warnings about the health of democracy certainly seem warranted, based on various measurements presented in this section.

According to the Polity IV regime dataset, and contrary to conventional wisdom, a greater number of countries have transitioned to democracies, which constitute a majority of nations worldwide. In 2000, 75 countries (52%) were governed democratically, 84 (57%) in 2010, and 90 countries (60%) in 2018.²⁷⁰ Additionally, the proportion of the global population living under democracy increased in absolute terms from 3.4 billion (57%) at the turn of the century to 4.3 billion (58%) in 2018. The number of states ‘stuck in the middle’, also referred to as anocracies, shows few changes, with 40 anocracies (28%) in 2000 and 39 (26%) in 2018.²⁷¹ However, the

270 Center for Systemic Peace, “Polity IV Project, Political Regime Characteristics and Transitions, 1800-2018,” Integrated Network for Societal Conflict Research (INSCR), July 27, 2019.

271 Patrick M. Regan and Sam R. Bell, “Changing Lanes or Stuck in the Middle: Why Are Anocracies More Prone to Civil Wars?,” 2010.

share of the population living under anocratic government rose from 715 million (12%) in 2000 to 1.3 billion (17%) in 2018.²⁷²

Foundational liberal norms of democratic regimes are under significant strain, with global levels of freedom declining, which will be discussed in more depth in the judicial section.²⁷³ Political scientists speak of “liberal democracy’s crisis of confidence,” reporting an increasing openness to non-democratic forms of governance (alongside still considerable levels of support for democracy).²⁷⁴ Others warn of a global “democratic deconsolidation,” with falling support for important democratic norms.²⁷⁵

Our measurements of individual support for democracies, using World Values Survey data and national voter turnout data, certainly lend some credence to these dire predictions. We find a decrease in the number of people expressing a desire to live in a democracy from 2005 to 2014. Global average voter turnout decreased from 68% to 61% between 2000 and 2018. Not only are individuals generally rating democracy less positively as a system; many of those who live under it are increasingly perceiving it as dysfunctional. Data from a 2018 Pew Research survey shows that 51% of respondents are dissatisfied with the way democracy works in their countries.²⁷⁶ This worrying trend reflects commonly held ideas of a ‘hollowing out’ of democracy at the state level,²⁷⁷ stemming from dissatisfaction with the system’s functioning. It may reflect a qualitative reduction of democracy that is not captured by a higher-level measurement such as Polity IV. There are notable regional differences that do not necessarily correlate with actual levels of democracy. Eastern European citizens, for instance, perceive their governments to be significantly less democratic than they often are.²⁷⁸ The negative nature of subjective measurements at the individual and state levels is partially tempered

272 Note: We filter out all nations with less than 1 million inhabitants in 2010 and exclude non-UN nations. Source: Center for Systemic Peace, “Polity IV Project, Political Regime Characteristics and Transitions, 1800-2018.”

273 Jay Ulfelder, “Global: More Democracy, Less Freedom,” Koto, January 19, 2018; Nate Schenkkan and Sarah Repucci, “The Freedom House Survey for 2018: Democracy in Retreat” (Journal of Democracy, April 2019).

274 Richard Wike and Janell Fetterolf, “Liberal Democracy’s Crisis of Confidence” (Journal of Democracy, October 2018).

275 Yascha Mounk and Roberto Stefan Foa, “The Signs of Deconsolidation” (Journal of Democracy, January 2017).

276 Richard Wike, Laura Silver, and Alexandra Castillo, “Many People Around the World Are Unhappy With How Democracy Is Working,” *Pew Research Center’s Global Attitudes Project* (blog), April 29, 2019.

277 Peter Mair, *Ruling the Void: The Hollowing out of Western Democracy* (New York City: Verso, 2013); Madeline Roache, “Central And Eastern Europeans Believe Democracy Is Under Threat, Poll Finds,” *Time*, April 11, 2019; Ursula Van Beek, ed., *Democracy Under Threat: A Crisis of Legitimacy?* (New York City: Springer, 2018).

278 Welzel, “WVS 1 to 6 Key Aggregates, Version 1”; Center for Systemic Peace, “Polity IV Project, Political Regime Characteristics and Transitions, 1800-2018.”

by the emergence of a (relatively) large number of pro-democracy movements in (among others) Algeria, Bolivia, Lebanon, Chile, Ecuador, Hong Kong, Iraq, Spain, Sudan, and Russia,²⁷⁹ but it is present within the data nonetheless. Finally, although an imperfect measurement at best, voting patterns in the United Nations General Assembly (UNGA) display a slight decline in disagreement between states between 2000 and 2018 of about 5%.²⁸⁰ This shows that at the system level states are able to reach consensus on a number of policy dossiers.




Overall, the answer to the question of whether the world has become more democratic is mixed, and on balance negative. Despite overall growth in the number of democracies, quite a few indicators are flashing yellow or red. The results of this analysis therefore paint a picture of a democratic world order under significant strain.

279 Francisco Serrano, "After 8 Months on the Streets, Protesters in Algeria Aren't Giving Up," *Foreign Policy* (blog), 2019; Yascha Mounk, "Bolivia Should Worry Autocrats Everywhere," *The Atlantic*, 2019; Kareem Chehayeb Sewell Abby, "Why Protesters in Lebanon Are Taking to the Streets," *Foreign Policy* (blog), 2019; Jimmy Langman, "From Model to Muddle: Chile's Sad Slide Into Upheaval," *Foreign Policy* (blog), 2019; Associated Press, "Ecuador Protests End after Deal Struck with Indigenous Leaders," *The Guardian*, October 14, 2019, sec. World news; Audrey Wilson, "China Warns Hong Kong After Weekend of Violence," *Foreign Policy* (blog), 2019; Isabel Coles and Ghassan Adnan, "Iraq, Rocked by Protests, Enters New Phase of Uncertainty After Premier's Resignation," *Wall Street Journal*, December 1, 2019, sec. World; Agencies, "Spanish Police Clash with Thousands of Catalan Protesters in Barcelona," *The Guardian*, October 27, 2019, sec. World news; "Rights Group: Deadly Attacks on Sudan Protesters Were Planned," *Al Jazeera*, 2019; Amy Mackinnon Standish Reid, "Russians Begin to Consider Life Without Putin," *Foreign Policy* (blog), 2019.

280 Using Bailey, Strezhnev and Voeten's 'ideal point' scale. While the UNGA's resolutions rarely produce real policies on important issues, the UNGA does function as a key stage where states can express their opinions on global issues. UNGA voting cohesion is frequently used in studies, such as: Michael A. Bailey, Anton Strezhnev, and Erik Voeten, "Estimating Dynamic State Preferences from United Nations Voting Data," *Journal of Conflict Resolution* 61, no. 2 (2017): 430–56; Michael A. Bailey and Erik Voeten, "A Two-Dimensional Analysis of Seventy Years of United Nations Voting," *Public Choice* 176 (2018): 3355; Madeleine O. Hosli et al., "Voting Cohesion in the United Nations General Assembly: The Case of the European Union" (ECPR Fifth Pan-European Conference, Porto, Portugal, 2010).

4.5 Judicial

Table 18 Has the world become more just?

	Observation level	Indicator	All available dates	2 most recent years	Time range
	Subjective	Perceived fairness	—	—	2005 - 2014
	Objective	Civil liberties	—	▲	2000 - 2017
	Subjective	Corruption Perceptions Index	▲	—	2012 - 2018
	Objective	Rule of law	▲	▲	2000 - 2018
	Subjective	Human Rights	▲	▲	2000 - 2019
	Objective	Illiberal states' influence	▲	—	2000 - 2016

Results in the judicial domain are relatively positive at the state level, but less so at the individual and system levels. Freedom House reported declines in political rights and civil liberties for the thirteenth consecutive year, occurring in not free, partly free, and free countries, including in consolidated democracies.²⁸¹ On the civil liberties index, 66 countries improved their score between 2000 and 2005, while 10 worsened. Between 2005 and 2018, this ratio was reversed, with 48 worsening and 15 improving. At the same time, several regions, most importantly Eastern Europe, show positive progress, with Poland and Hungary being exceptions to this rule. These developments certainly provide greater context for the democratic trends discussed earlier, and are an additional cause for concern. Alongside these developments, the degree to which individuals perceive their peers as acting fairly in daily life remains more or less stable over time. Interestingly, more corrupt countries score significantly lower in perceived fairness than countries where corruption is less prevalent.

²⁸¹ Freedom House, "Freedom in the World 2019: Democracy in Retreat," Freedom in the World 2019, January 15, 2019.

At the level of states, the Corruption Perception Index (CPI) shows a slight but positive increase in the levels of confidence in the functioning of national legal systems as expressed in expert assessments and business opinion surveys.²⁸² Positive developments are reported in countries in Eastern Europe (again with Hungary and Poland as an example of the opposite trend) and negative developments in the Middle East. The transparency and independence of the rule of law exercised at the state level has also seen moderate improvements over the past decades based on data from the V-DEM's Rule of Law Index, which considers factors such as independence of the judiciary, transparency of laws, predictability of legal enforcement, access to justice, and governmental officials' compliance with the law.²⁸³

Most Western states tend to have strong rule of law records and have remained more or less stable in the upper ranges. Other regions trail far behind the West, with Africa and the MENA region scoring particularly low and Latin America, the Caribbean, Asia, and the Pacific in the mid-ranges. Eastern Europe has average rule of law scores that are closer to those in Latin America than in western European states. Rule of law correlates significantly both with democratic regime type (as measured by Polity IV) and with civil liberties (as measured by Freedom House), because liberal democratic states by definition have stronger legislative and judicial institutions which are independent of the executive.²⁸⁴ There are a number of important exceptions, however, with the rule of law being rigorously enforced in a small number of illiberal authoritarian states such as the United Arab Emirates, Oman, and Kuwait, as well as the anocratic Singapore, all nations that are wealthy and/or highly integrated into global markets.

There is no authoritative dataset that systematically measures human rights violations. According to a composite index measurement combining several human rights indicators, governments' records in respecting and protecting human rights have been improving in almost all regions except the MENA over the past two decades.²⁸⁵ At the same time, human rights protection organizations have reported increases in human

282 "Corruption Perceptions Index 2018," Transparency International, 20, accessed December 11, 2019; "Corruption Perceptions Index 2018: Technical Methodology Note" (Transparency International, 2018).

283 Michael Coppedge et al., "V-Dem Codebook V9" (Varieties of Democracy (V-Dem) Project, 2019).

284 See for example Coppedge et al.; "Methodology 2019," Freedom House, January 15, 2019. Both at a statistically significant level of $p < 0.0001$, not controlling for other variables.

285 The dataset used here is "Latent Human Rights Protection Scores Version 3" (v3.01, 2019–05–28), first developed by Schnakenberg and Fariss (2014) and subsequently updated by Fariss (2019). The Latent Human Rights Protection Scores—which we simply call Human Rights Scores here—have values from around –3.8 to around 5.4 (the higher the better). Indicators used are binary variables on: torture, government killing, political imprisonment, extrajudicial executions, mass killings and disappearances. To construct the Human Rights Scores, Fariss (2019) uses data from nine sources. For more information see Christopher Fariss, "Yes, Human Rights Practices Are Improving Over Time," May 27, 2019.

285 Fariss.

rights violations by governments. In recent years, the world has seen blatant human rights violations in wars, such as those in Syria and Yemen, as well as domestically, for example in China and Egypt.²⁸⁶ While this is a complex issue, research underlying the composite index suggests that over time human rights protections have improved, but so have the standards in measurements used to assess progress.²⁸⁷

A final worrying trend to report at the system level is the fact that illiberal states continue to increase their international influence. Data from Freedom House and the Frederick S. Pardee Center for International Futures show that illiberal states are gaining in political, economic, and military influence. The emerging international order is shaped by this process, partly replacing the Western-led liberal democratic model. Illiberal states such as China are extending their geopolitical influence through projects such as the Asia-Pacific Economic Cooperation summit,²⁸⁸ the Asian Infrastructure Investment Bank, and of course the Belt and Road Initiative.²⁸⁹ Other autocratic regimes similarly reject the Western order, succinctly captured by Vladimir Putin's assertion in the summer of 2019 that liberalism is "obsolete."²⁹⁰ While the rise in illiberal states' influence shows a slight stagnation toward the end of the data in 2016, the trend reflects their centrality within the international system and their growing ability to shape international norms and rules.

Overall, to the question of whether the world has become more just, there is, unsurprisingly, not a straightforward answer, because of different and often contradictory developments taking place at the individual, state, and system levels. The picture that emerges from our analysis is not positive for the state of freedom in the world: in the domestic arena, freedom has been declining for over a decade; in the international arena, illiberal values are becoming more dominant.

286 Rodrigo Campos, "Human Rights Chief Slams Security Council for Inaction on Syria," *Reuters*, March 20, 2018; Roald Høvring, "10 Things to Know about the Crisis in Yemen," NRC, accessed November 25, 2019; Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," Council on Foreign Relations, November 25, 2019; "World Report 2019: Rights Trends in Egypt," Human Rights Watch, January 17, 2018.

287 Keith Schnakenberg and Christopher Fariss, "Dynamic Patterns of Human Rights Practices," *Political Science Research and Methods*, April 2014; Fariss, "Yes, Human Rights Practices Are Improving Over Time."




288 Christopher Walker et al., "Sharp Power: Rising Authoritarian Influence" (National Endowment for Democracy and the International Forum for Democratic Studies, May 12, 2017).

289 David Dollar, "The AIIB and the 'One Belt, One Road,'" *Brookings* (blog), June 21, 2015.

290 Matt McGrath, "Putin: Russian President Says Liberalism 'Obsolete,'" *BBC News*, June 28, 2019, sec. Europe.

4.6 Security

Table 19 Has the world become more peaceful?

	Observation level	Indicator	All available dates	2 most recent years	Time range
	Subjective	Willingness to fight	—	—	2000 - 2014
	Objective	Conflict fatalities	▲	▼	2000 - 2018
	Subjective	Negative military rhetorical assertiveness	▲	▼	2000 - 2019
	Objective	Military expenditure	—	▼	2000 - 2018
	Subjective	Global Peace Index	▲	▼	2008 - 2018
	Objective	Number of active conflicts	▲	—	2000 - 2018

The past few decades have seen a worrying overall increase in insecurity across a range of dimensions and at multiple levels. Far from representing a global trend, however, a few flashpoints and highly violent conflicts have significantly driven up global fatality numbers according to data from the Uppsala Conflict Data Program.²⁹¹ Since the lowest point in 2010, the number of violent state-based conflicts has risen from 30 to 52. Similarly, the number of one-sided conflicts steadily increased over the past decade, reaching a record of 35 conflicts last year – a substantial increase from 21 conflicts ten years ago. Although fluctuating between years, the number of non-state conflicts increased most significantly, from 28 conflicts in 2010 to 78 violent incidents in 2018. Together with this, the number of conflict-related deaths increased from 30,867 in 2010 to a peak of 143,409 in 2014. The past two years saw a 27% decrease in global death tolls, with 106,557 in 2016, 95,500 in 2017, and 77,392 in 2018, which nevertheless remain far (150%) above pre-2010 levels.²⁹² Particularly the MENA region as a whole, and the conflicts in Libya, Yemen, and Syria in particular, contributed to this trend. Recent years have seen a reduction in absolute levels of violence in the region, even if the

291 Ralph Sundberg and Erik Melander, “Introducing the UCDP Georeferenced Event Dataset,” *Journal of Peace Research* 50, no. 4 (2013): 523–32.

292 “UCDP - Uppsala Conflict Data Program.”

humanitarian situation in Yemen remains abhorrent, Libya features persistent fighting between warring factions, and the war in Syria has not fully ended yet. Renewed popular unrest in this unstable region²⁹³ and the looming threat of the conflict trap (60% of the conflicts from the early 2000s relapsed in the following five years) do not necessarily bode well for future trends in conflict fatalities.²⁹⁴

Meanwhile, willingness to fight, as registered by World Values Survey data, has remained stable at an overall level, although there are clear variations. Approximately 70% of the respondents answered affirmatively when asked whether they would be willing to fight for their country if war broke out. Above all, citizens of high-income countries are decidedly less willing to fight (62%) than those residing in countries with lower income (80%).²⁹⁵ Research suggests that an abundance of life opportunities reduces individuals' willingness to die for their country.²⁹⁶ A related argument posits that people are less likely to sacrifice their life once they have obtained a certain material and social status. Readiness to fight for one's country is lowest in Western Europe (25%) and highest in the MENA region (83%).²⁹⁷

At the interstate level, our analysis of the use of military threats did not find any increase at the global level, as reported in chapter 2.1 on military competition. But a number of high-profile threats by political leaders of the dominant military powers are a cause of concern, and overall levels of military assertive rhetoric have even increased slightly. While global military spending has remained stable at around 2.3% of GDP since the 2000s, absolute levels of military spending have increased by 13.2% over the past decade and now amount to \$1.78 trillion in total. With the number of active conflicts increasing at the system level, the global level of peacefulness has decreased by 3.8% since 2008, according to the Global Peace Index (GPI).²⁹⁸ The level of peacefulness in the world has declined in eight of the last twelve years. Regionally, Europe continues to be the most peaceful region in the world, with 22 out of 36 European countries ranking

293 Michael Safi, "Frustration and Anger Fuel Wave of Youth Unrest in Arab World," *The Observer*, November 2, 2019, sec. World news.

294 Sebastian von Einsiedel, "Civil War Trends and the Changing Nature of Armed Conflict," *United Nations University*, 2017; Collier, Paul et al., "Breaking the Conflict Trap : Civil War and Development Policy" (World Bank, 2003).

295 Gallup International Association, "Voice of the People 2015," 201, accessed December 9, 2019.

296 Ronald F Inglehart, Bi Puranen, and Christian Welzel, "Declining Willingness to Fight for One's Country: The Individual-Level Basis of the Long Peace," *Journal of Peace Research* 52, no. 4 (March 7, 2015): 418–34.

297 Gallup Pakistan, "WIN/Gallup International's Global Survey Shows Three in Five Willing to Fight for Their Country," Press Release, March 18, 2015.

298 Institute for Economics and Peace, "Global Peace Index 2019," 2019, 201.

higher on the GPI index this year than they did previously. Due to its numerous intra- and interstate conflicts, the MENA ranks as the least peaceful region globally.²⁹⁹

Overall, when measured over the entire period, the world has not become more secure. Our analysis records higher numbers of conflicts and conflict fatalities and declining levels of peace over the past two decades. While military expenditures as a percentage of GDP have remained similar, absolute levels have been increasing, especially in the case of major military powers. There are some positive developments in recent years, particularly in the reduction of conflict fatalities over the past two years, but the situation in key conflict hotspots is no reason for excessive optimism. The answer to the question of whether the world has become more secure is therefore negative.

4.7 Sub-conclusions

As is to be expected in a world with over seven billion inhabitants living across seven continents, with different cultures and societies at very different levels of socio-economic development, our analysis, even at the system level, presents a kaleidoscopic picture. Yet at this very macro level, our analysis warrants the following conclusions.

First, the global population as a whole has become more prosperous. Progress has certainly not been limited to the rich: the world's poor continue to see significant improvements in living standards. Although inequality between states has been decreasing globally because of the Rise of the Rest, levels of inequality within states have worsened according to various measures. The overall level of global inequality is still higher than the level of inequality of countries with the highest levels of domestic inequality.

Second, and unsurprisingly, the world continues to become more connected, both physically and virtually. Various measurements show increases at the level of individuals, states and the system as a whole for, among others, informational connectedness, trade, diplomatic, and social interaction. Stagnating growth is nevertheless recorded in the level of globalization, while trust among individuals in fellow citizens has decreased over the entire period. Although the world has become more connected, increased connectivity has not necessarily brought the world closer together.

Third, the world has not become more inclusionary, although that claim warrants some caveats. Alongside a marked surge in identity-driven politics in both developing and consolidated democracies, measurements of inclusiveness show a negative trend. This is despite more recent increased awareness of gender and racial issues. States have been

²⁹⁹ Institute for Economics and Peace, 201.

curbing religious freedoms, and social hostilities over religion have increased over the entire period. Taking into account the lack of up-to-date, granular data on in-group/out-group dynamics, the prevalence of exclusionary dynamics at different levels is a cause of concern.

Fourth, despite overall growth in both the number of democracies and the absolute number of citizens living in democracies, democracy as an institution is under attack. Democracy is no longer considered to be a regime type of choice by many. Frequently heard warnings about the health of democracy seem justified based on growing openness to other forms of governance, falling support for democratic norms, and lower national voter turnout. Yet the pro-democracy movements from Bolivia to Algeria and from Russia to Hong Kong do show that democracy continues to appeal to many.

Fifth, the picture in the closely associated realm of justice is also multilayered. Freedom understood in terms of civil rights has been declining for over a decade now, in both free and unfree countries. Human rights are under pressure, with horrific human rights violations occurring in a wide range of countries. Recent research nevertheless suggests that human rights protections have also steadily improved over time. The rule of law, meanwhile, has strengthened over the past decades, although many states started from very low baselines. A disquieting development is the fact that illiberal states have been gaining in political, economic, and military influence, which is likely to translate into their growing ability to shape international norms and rules.

Finally, when measured over the past two decades, the world has not become more peaceful and secure overall. The world has seen a growing number of conflicts and conflict fatalities combined with declining levels of peace over the past two decades. On a positive note, the past two years saw a reduction in the number of conflict fatalities, but the medium-term outlook for conflict zones does not provide solid grounds for excessive optimism.

5 The Netherlands in the World

In the context of shifts in global power distribution, the position of the Netherlands is shifting too. The US' "abdication of global leadership",³⁰⁰ in combination with China's rapid ascent to great power status, puts a strain on the international community's ability to find consensus on a range of pressing international dossiers. These include climate change action (e.g., the Paris Climate Agreement),³⁰¹ nuclear counter-proliferation efforts (Iran and the now *de facto* defunct JCPOA),³⁰² arms control (e.g., the dissolution of the INF Treaty), free trade (the series of trade disputes between the US and China but also with the EU),³⁰³ the wars in the Middle East (the US' sudden partial withdrawal from Syria, the roles of Russia and Iran, and the conflict between the US and Iran). In this environment, middle powers, either alone or in coalitions with other middle powers, continue to work on global dossiers to achieve their foreign policy objectives, as we already described in last year's report.³⁰⁴

Navigating this changing global environment requires first and foremost a keen understanding of changes in Dutch foreign relations. The Dutch Foreign Relations Index (DFRI), developed by HCSS, captures the relationship between the Netherlands and other countries over time through a quantitative measurement of a limited set of important dimensions in international relations. The DFRI differentiates between relevance ("how important is this country for the Netherlands and the international sphere?") and compatibility ("to what extent does this country share similar values and goals to the Netherlands?"). The two dimensions thus align neatly with two key tenets of Dutch foreign policy: interests and values. The DFRI operationalizes these dimensions through four key domains of international politics: political, military, economic, and judicial, and collects data for all these measurements for the period between 1996 and the present. Combining interests and values provides a multidimensional picture of

300 Ivo H. Daalder and James M. Lindsay, *The Empty Throne: America's Abdication of Global Leadership* (New York: Public Affairs, 2018).

301 Emily Holden, "Trump Begins Year-Long Process to Formally Exit Paris Climate Agreement," *The Guardian*, November 5, 2019, sec. US news.

302 Dan Smith, "The US Withdrawal from the Iran Deal: One Year on | SIPRI," *SIPRI* (blog), May 2019.

303 Christiaan Pelgrim and Clara van de Wiel, "Handelsconflict VS En EU Bedreigt Wereldeconomie," *NRC*, October 2019.

304 Willem Oosterveld and Bianca Torossian, "A Balancing Act | Strategic Monitor 2018-2019" (HCSS, December 2018).

the Dutch position vis-à-vis other countries. This can subsequently help in identifying potential partners as well as potential adversaries in the pursuit of Dutch foreign policy objectives.

The DFRI is also a useful instrument in the further development of a longer-term Dutch government vision of foreign policy. The Dutch government coalition agreement of October 2017 delineated a set of foreign policy goals for the next four years. The agreement expressed the coalition's intention to pursue "a realistic foreign policy that serves both Dutch interests and the international rule-based order."³⁰⁵ It proposed a security strategy that integrates national and international security challenges, a strategy that was published in 2018.³⁰⁶ It pledged to work through international organizations such as the EU, NATO, and the UN. It sought to focus on neighboring EU countries and Europe's "ring of instability." It committed to increasing the defense budget, strengthening the Dutch armed forces and establishing closer military partnerships with "like-minded countries." The coalition's plans foreshadowed important decisions about the countries with which the Netherlands is actively seeking closer or less close relationships. New directions will be set in the drafting of the updated integrated security strategy and the Defense Vision, both scheduled for 2020, and the next coalition agreement after the 2021 elections.

A word of caution is in order: like any other index, the DFRI provides a first high-level overview in this particular case of the state of Dutch foreign relations, based on a select number of indicators for which data have been collected, collated, and combined. The selection and combination of these indicators are described and explained in a longer method document (see also Table 20).³⁰⁷ The DFRI considers dyadic relations, which means that it looks at relations between the Netherlands and third countries. It does not consider the position of the Netherlands in the global web of international relations, which would mean also taking into account the relations of the Netherlands in the context of the bilateral relations of other countries. The latter would provide greater context and depth to an analysis of its position, particularly in a multi-order world. Furthermore, this chapter provides only a concise and straightforward description of the results of the index. Further triangulation and contextualization of these results based on the analysis of secondary sources and qualitative in-depth assessment would be beyond the scope of this year's report. This will happen in the Strategic Monitor 2020–2021,

305 VVD, CDA, and D66 en ChristenUnie, "Regeerakkoord 'Vertrouwen in de toekomst' - Publicatie - Kabinetsformatie," Bureau Woordvoering Kabinetsformatie, October 10, 2017.

306 "Wereldwijd Voor Een Veilig Nederland: Geïntegreerde Buitenland- En Veiligheidsstrategie 2018-2022" (The Hague: Ministerie van Buitenlandse Zaken, 2018).

307 For a more detailed description of the indicators and underlying data, issues, please refer to the DFRI Methodology Document, Hugo van Manen et al., "Methodological Note - The Dutch Foreign Relations Index: Version 2" (The Hague Centre for Strategic Studies, January 2020).

in which a standalone research project will be devoted to the state of Dutch foreign relations and the role of the Netherlands in the global web of foreign relations. Readers of this chapter should therefore not overinterpret the results reported here and should note that further analysis and contextualization will take place on the basis of these first high-level results in next year’s report.

Table 20 Relevance and compatibility: indicators, definitions, and sources of the DFRI

Domains	Dimensions	Description	Proxy	Source
Political	Relevance	Measurement of a state’s influence within the global system.	Foreign Bilateral Influence Capacity Index	Pardee Center for International Futures: The Global Influence Index
	Compatibility	Measurement of the degree to which the Netherlands and country X share membership in international organizations, exchange diplomatic missions, and express similar foreign policy preferences.	Shared membership of IGOs, Diplomatic Representation & United Nations General Assembly Voting Behavior	Pardee Center of International Futures: Political Bandwidth & United Nations General Assembly Voting Data
Military	Relevance	Measurement of a state’s military coercive capabilities.	Share of global power	Pardee Center for International Futures: Global Power Index
	Compatibility	Measurement of the depth and intensity of military alignment and cooperation	Shared alliances, shared Centers of Excellence within NATO or other (non-EU) multilateral military cooperation platform (e.g., MNFP), as well as instances of training or procurement outside of NATO or EU frameworks.	NATO/EU & CoE websites. Notes to Parliament from the Dutch Minister of Defense (2012-2019)
Economic	Relevance	Measurement of a state’s importance to the Dutch economy.	Bilateral import and export volume with the Netherlands	UN Comtrade

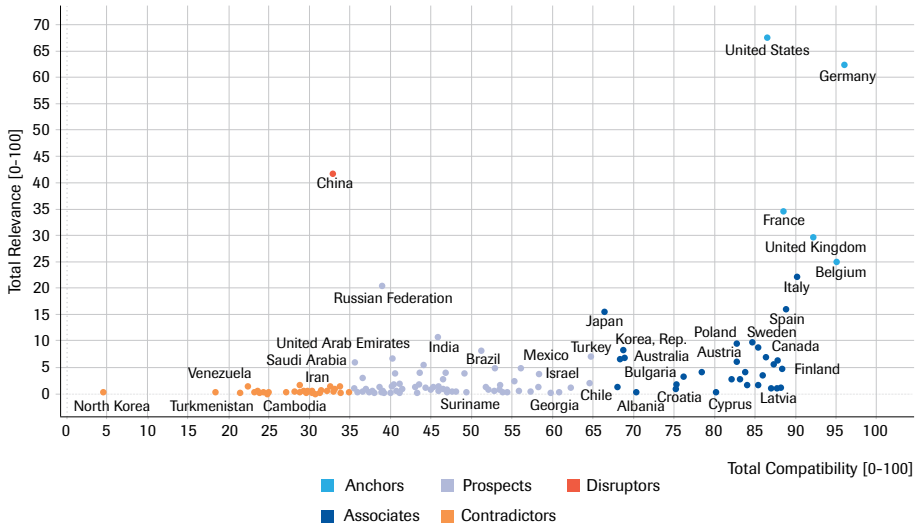
Domains	Dimensions	Description	Proxy	Source
	Compatibility	Measurement of the similarity in the way in which the Netherlands and country X value the principles of free trade.	Regulatory regimes concerning domestic business, labor, and monetary regulation, as well as trade, investment, and finance regulations	Selected measures from the Economic Freedom Index
Judicial	Relevance	Measurement of a state's ability to influence international norms and norm-making processes.	Global Influence (same as political relevance) ³⁰⁸	
	Compatibility	Measurement of distance between the degree to which the Netherlands and country X subscribe to liberal democratic principles.	Level of electoral democracy and effective checks and balances on executive power	V-DEM Liberal Democracy Index

308 The ability to contribute significantly to international norm-making is hard to meaningfully separate from the ability to shape international political decision-making in general, leading the DFRI to use political relevance as the proxy for judicial relevance. This is only for purposes of within-domain analysis of relevance and compatibility, however. In the total relevance scores, judicial was excluded, as its inclusion would simply mean counting political relevance twice.

5.1 The Netherlands and Foreign Relations

Mapping countries on the relevance and compatibility dimensions yields five different clusters of countries (see Figure 2): *anchors*, *associates*, *prospects*, *contradictors*, and *disruptors*.³⁰⁹

Figure 2 Relevance (y-axis) and Compatibility (x-axis) for all countries



The most fundamental of these we call *anchors*. Anchor states from the Dutch perspective are neighboring states, regional economic powerhouses, and the world’s largest military power. These states are both highly relevant for and highly compatible with the Netherlands. They are important states for a mixture of political, military, and economic reasons, and share largely similar worldviews. These states (the US, Germany, France, the UK, and Belgium in 2018) constitute important countries in the dimensions measured by the DFRI. Most of these countries are important international actors, comprising three UNSC members and four of the ten largest economies of the world. Belgium’s presence is explained through its proximity, and the close cooperation between the Netherlands and Belgium along a number of important dimensions,

309 These categories are established mathematically: the distinction between the high-relevance categories (Anchors and Disruptors) and the others was made by dividing the highest relevance-score in 2018 (67.49) by three, meaning the boundary became 22.5. The compatibility categories were made in a similar manner, namely by subtracting the lowest compatibility score in 2018 (4.59) from the highest (96.12) and dividing that range into three equal parts (of 30.51 points each). The Disruptor-Anchor dichotomy was made by dividing this same range by two.

including the economic and military dimension. For now, the question remains whether Brexit will drastically affect the relevance and compatibility of the United Kingdom, although it will inevitably have an economic impact and will change the dynamics within the European Union.³¹⁰

The second cluster of *associates* comprises liberal states that are either European Union member states or fall under the US security umbrella, with low to medium degrees of relevance scores on the DFRI. The associate category includes the Scandinavian countries, transitioned (eastern) European states, southern European states (Italy, Spain and Portugal), Commonwealth countries such as Australia and Canada, and two East Asian states: South Korea and Japan. Many of the associates possess very high potential relevance and could well become anchors if relations were to deepen. Considering the sizes of their economies, ties with states such as Canada, Japan, and South Korea could be strengthened, which would propel them into the anchor category. Despite the negative developments on the liberal democratic front in recent years, Hungary and Poland are still part of the associates group. Turkey, however, has moved further away.

The third cluster, *prospects*, consists of states that, with the exception of some (Russia and India in particular), have varying degrees of relevance as measured by the indicators in the DFRI, while their values systems do not necessarily align with those of the Netherlands. This category contains the largest number of states. It includes Western-aligned but highly authoritarian countries like Saudi Arabia and the United Arab Emirates, both of which were in the contradictor category until recently on the basis of their DFRI scores, but it also features non-European democratic states such as Israel. This category contains important non-Western states, such as Russia, which is very nearly a disruptor, although its relevance score in the DFRI decreased after the oil price crash and the introduction of sanctions by the EU in 2014.³¹¹ It also includes many emerging powers such as India and Brazil. While they may not be first choices for close partnerships, these states may certainly be amenable to cooperation in specific dossiers that are relevant to Dutch foreign policies, especially in the higher compatibility range of this category. In certain geographic regions where Dutch anchors or associates have limited influence, such cooperation may be particularly useful, for instance in the Indian Ocean theater, in which India's role could be important in the ensuing rivalry between the US and China.

The cluster we label *contradictors* contains states which are at the far extreme of the economic, political, and judicial spectrum relative to the Netherlands. Contradictors include internationally isolated countries such as Iran and Venezuela, and/or the

310 See for instance “Forming Coalitions in the EU after Brexit: Alliances for a European Union That Modernises and Protects,” publicatie (Advisory Council on International Affairs, July 6, 2018).

311 “EU Sanctions Map: Russia,” European Commission, July 2019.

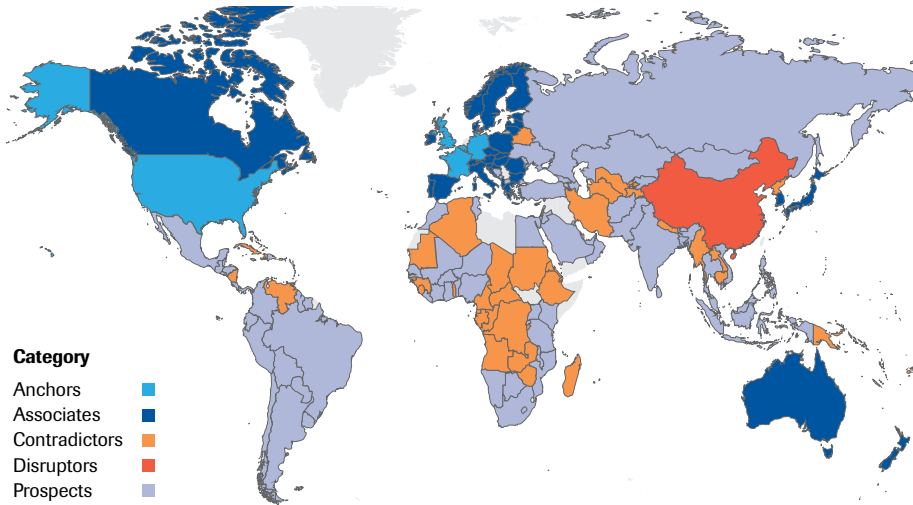
world's harshest dictatorships, such as North Korea and Turkmenistan. These states are economically and politically illiberal. Because of this they also include many lesser developed states, including in Africa. Contradictors' outright incompatibility with the Netherlands, their frequent status as international pariahs, and often underdeveloped economy, also mean that many of these states are ranked lower in terms of relevance.

Fifth, and finally, is the *disruptor* category, which involves highly relevant countries whose value systems are at the same time very different from the Netherlands. These states have sufficient global influence to shape significant international regimes, yet their values diverge from Dutch values in the areas of democracy and human rights, the role of governments in the regulation of economies, and the international rule of law. This does not mean that these states should be avoided. On the contrary, they may even require additional outreach efforts. In 2018, the only state in this category was the steadily rising China. While Russia continues to be a high foreign policy priority (with comparatively much higher scores than other contradictors), China is both more dissimilar to the Netherlands and more powerful than Russia. Its rise has been marked by economic as well as military strength, but its closer integration in the global economy has not led to an assimilation of Western liberal ideas and values. While this does not necessarily conflict, a high reliance on a very different type of state is a liability that the Netherlands has started to actively engage with – for example, through the discussion on Chinese companies' contribution to 5G infrastructure – and will undoubtedly do so in the years to come.³¹²

There are clear geographic clusters of country types (see Figure 3). The anchors and associates clusters are European or Anglo-Saxon countries, complemented by South Korea and Japan. The only NATO countries not in this category are Montenegro, a recent addition, and Turkey, whose illiberal domestic developments as well as its international antagonism to its Atlantic partners has been cause of concern for a number of years now. The prospects, the largest group, are dispersed globally. The contradictors consist of the highly illiberal, authoritarian states, the majority of which are on the African continent. The sole disruptor is China.

312 "Huawei Mag Meebouwen Aan 5G-Netwerken in Duitsland," *NOS*, October 14, 2019.

Figure 3 Map of the five different categories in 2018

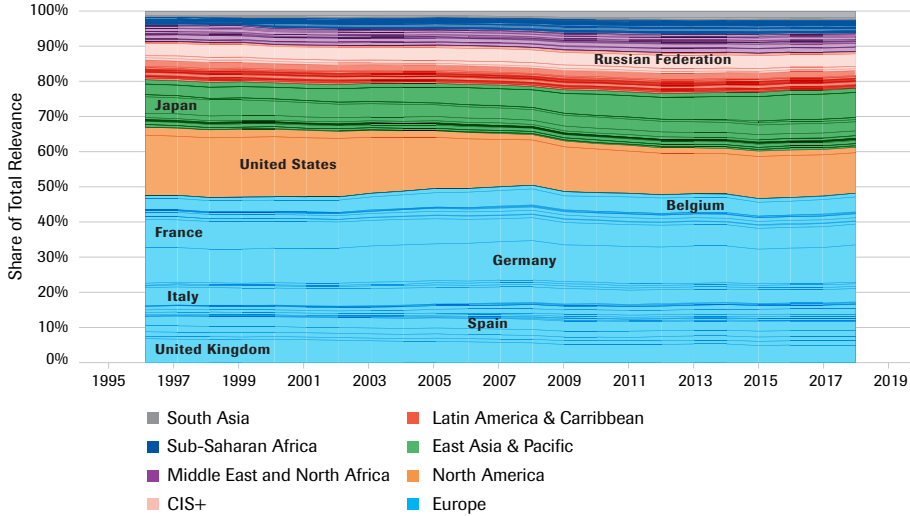


Over the last twenty years, Dutch relations with other countries have improved according to the DFRI. One could even say that from the perspective of Dutch foreign relations the Netherlands finds itself in a fortuitous position. The Netherlands is surrounded by anchors and associates. The total number of associates has doubled to 30 since 1996. There are also fewer dissimilar states, as the number of contradictors has fallen by fifth to 39. Importantly, these countries are now almost exclusively located in Africa. Many of the countries in the European neighborhood, in the Middle East, and in the former Soviet sphere have become more likely partners – prospects – for the future. A few populous Asian nations such as Vietnam and Indonesia have gone through similar developments. Both in these theaters and elsewhere, opportunities for cooperation have appeared for the Netherlands.

The roles of North America, Europe, and Asia have changed in recent decades, with the former stagnating in importance and the latter two growing in relevance. It should come as little surprise that North America and Europe are the most compatible regions in the world. Europe’s relevance to the Netherlands is only increasing. This is despite the fact that the 2008 economic crisis and the 2014 decline in trade appear to have affected mainly the relevance of this region, while leaving others largely unscathed.

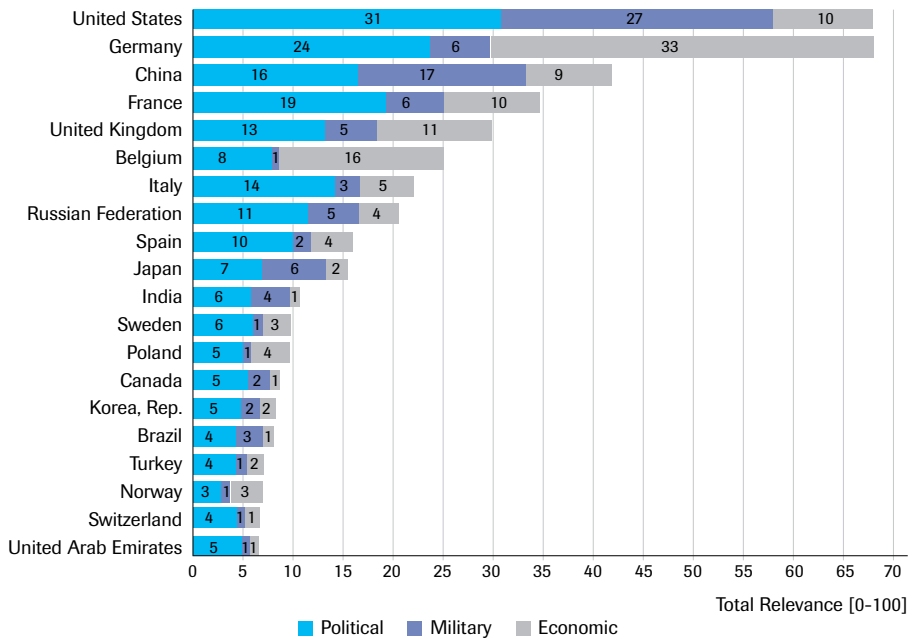
5.2 Which States are the Most Relevant?

Figure 4 Share of total relevance per country and region over time



In relative terms, Europe remains at the core of Dutch foreign relations, but the US and Canada are ceding ground to emerging powers, notably China. Europe's share of overall relevance remains stable at around half. The relevance of the UK, France, and Italy decreased while that of Belgium, but especially Germany, increased. China's rise is spectacular, more than doubling its share of relevance due to growth in economic, political, and military relevance. Vietnam is also a notable riser, as its relevance has nearly quintupled, making it now comparable to European states such as Portugal or Greece. Prospects that have grown significantly in military and political relevance are Saudi Arabia and the UAE, but Russia has also become more relevant. Turkey poses a complicated case, as its significant rise in relevance is matched, as we will see, by a significant decrease in compatibility. Despite these dynamics, the dominant partners of old, the US and Germany, remain just that, although the dominance of the US has decreased significantly over the past decade (see Figure 4 and Figure 5).

Figure 5 Highest scores in total relevance in 2018, broken down by domain



The total number of countries decreasing in relevance, as well as the degree by which they decreased, is far lower than the countries that increased (see Figure 6 and Figure 7). This is due to the fact that relevance (with the exception of military relevance) is not a zero-sum game and particularly the total level of economic relevance – Dutch bilateral trade – rose overall in the period under review.³¹³ It is no surprise, then, that the most dramatic decreases are in military and political relevance.

313 An effect which would be even greater if 2008 or 2009 were taken as a baseline.

Figure 6 Top 20 biggest increases in total relevance between 2007 and 2018, broken down by domain

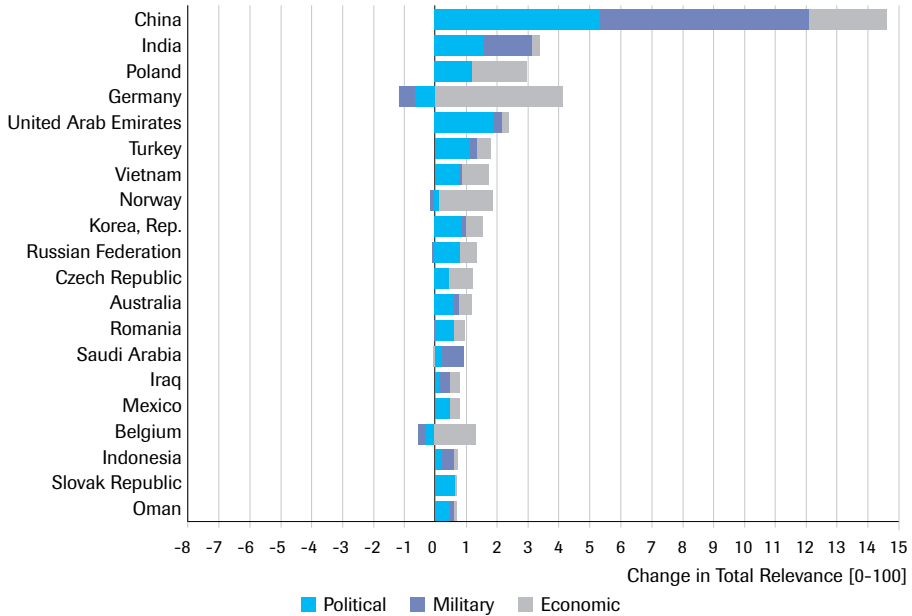
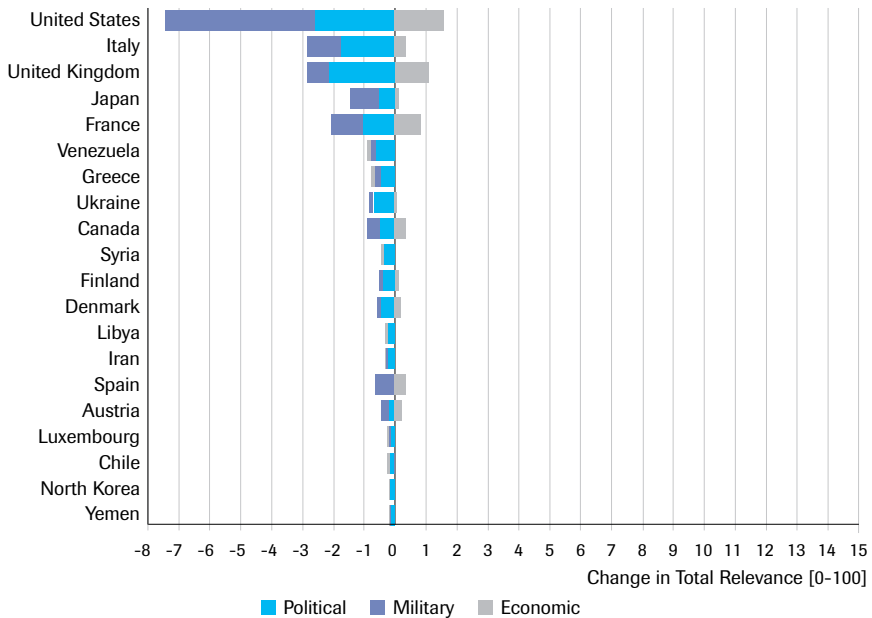


Figure 7 Top 20 biggest decreases in total relevance between 2007 and 2018, broken down by domain



Almost all of the top declining countries are close allies of the Netherlands. This is a reflection of the globally changing balance of power. The rise of powers such as China on the military front has led to a relative reduction in military and political relevance for many of the world's traditional powerbrokers, such as the US, the UK, and France. The international status quo, of which the Netherlands has traditionally been a firm supporter, has been upset by the rise of new powers, and the Dutch allies are less relevant because of this development.

This trend is further underlined by the relative decline of NATO's military relevance. Until 2013, the states in NATO together possessed more military power than all other states in the world combined as measured by the military relevance indicator of the DFRI, which is based on the Global Power Index of the Pardee Center for International Futures. This was despite the fact that in terms of number of countries, NATO was outnumbered 10 to 1 in 1995 and 5 to 1 in 2018.³¹⁴ NATO's dominance has declined steadily throughout this period, however, and increasingly so since 2008. First surpassed in 2013, NATO states together now account for less than half of the world's military power. The era of NATO's unassailable military superiority is over and continues to face a downward trend.³¹⁵ Aside from a slight rise in Poland and Turkey, no NATO country has risen in military relevance since 2007. As this measure is indexed as a zero-sum game, this can largely be explained by the rise of previously lesser military powers. These include Arab states such as the UAE and Saudi Arabia, but also India and China. China is single-handedly responsible for a large portion of the rise of non-NATO countries, as its power doubled between 2003 and 2018. The US alone still possesses a quarter of global military power, with China at less than one-sixth. Contrary to the US, however, China's relative power is increasing.

5.3 Which States are the Most Compatible?

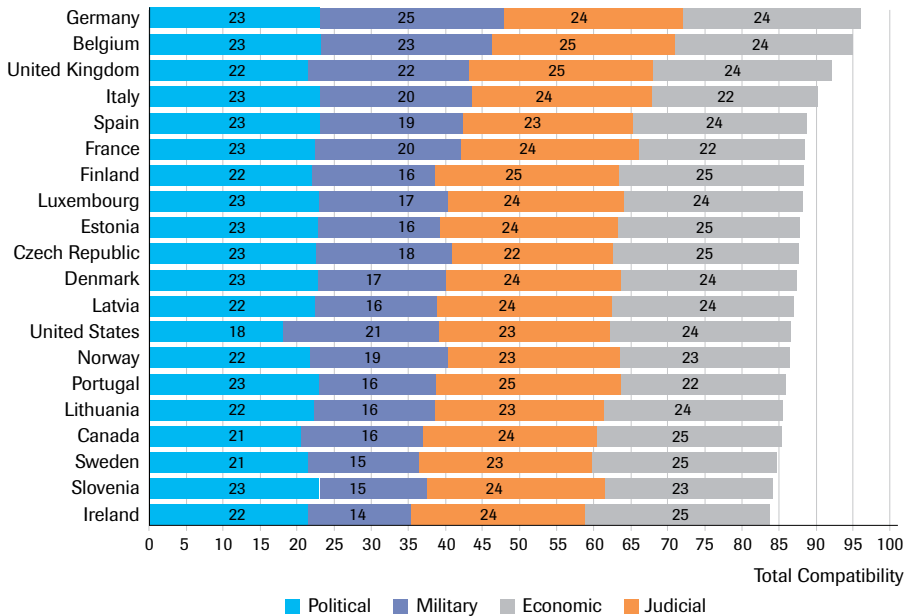
The top twenty of countries whose value systems are most aligned with the Netherlands consists only of European and North American states (see Figure 8). This should come as no surprise because of close and longstanding ties with the states in regions with strongly institutionalized forms of cooperation. The trend that emerges from this list is remarkably stable. Nearly all nations have near-perfect scores in terms of judicial, economic, and political similarity with the Netherlands, showing that it is firmly integrated in a regional system of like-minded states.³¹⁶

314 With a population of over 500,000 in 2010. If you were to consider population ratios, this is 12.5% in 1995 and 12.3% in 2018, a 1:8 ratio.

315 A clash between NATO and all non-NATO members working in unison is of course entirely fictional. The extent of the US' security umbrella includes many countries outside of NATO such as Japan, South Korea, and Australia, all three of which are enough to shift the total power balance back into NATO's favor. Nor are all nations outside of this umbrella a unified front – far from it.

316 Mohammed Haddad, Usaid Siddiqui, and Owais Zaheer, "How Has My Country Voted at the UN?," Al Jazeera, accessed December 9, 2019.

Figure 8 Highest scores in Compatibility in 2018, broken down by domain



Unlike the relevance dimension, the highest increases in compatibility with the Netherlands are found among existing allies and democratizing non-Western states (see Figure 9). One group is made up of European states with which military coordination has increased in recent years, in the context of the EU, NATO, or through bilateral cooperation. Another group consists of prospects or even contradictor states that have been going through a process of economic and political liberalization and, albeit sometimes very checkered, improvements in the protection of their human rights record. Most notable in this group are Tunisia, Myanmar, and Gambia. Increases in the political compatibility domain indicate that states are sharing a greater number of overlapping memberships in international organizations and are more in agreement with Dutch foreign policy objectives. It is clear that this political compatibility does not necessarily align with judicial compatibility, as examples such as the UAE and Qatar demonstrate. Increases in political compatibility therefore represent an opportunity for increased functional cooperation on international political issues.

Figure 9 Top 20 states with largest increases in terms of total compatibility, broken down by domain

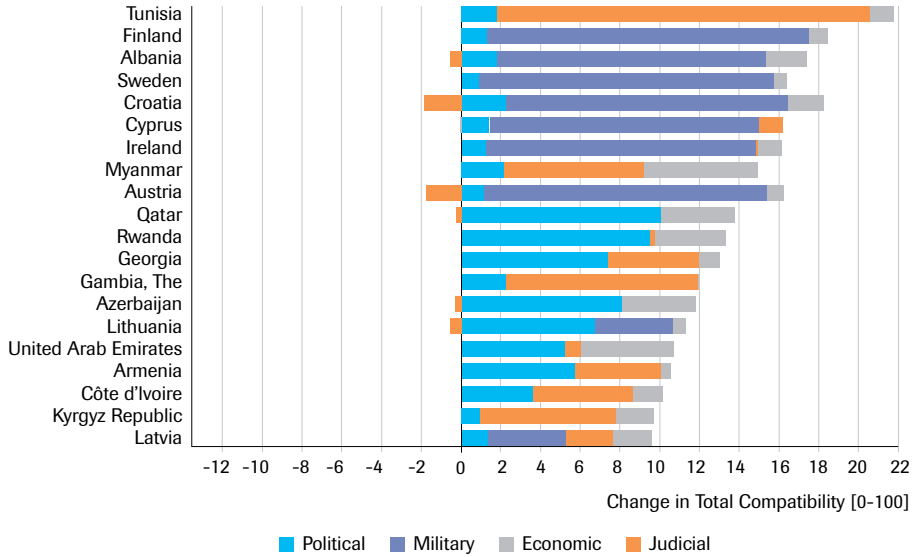
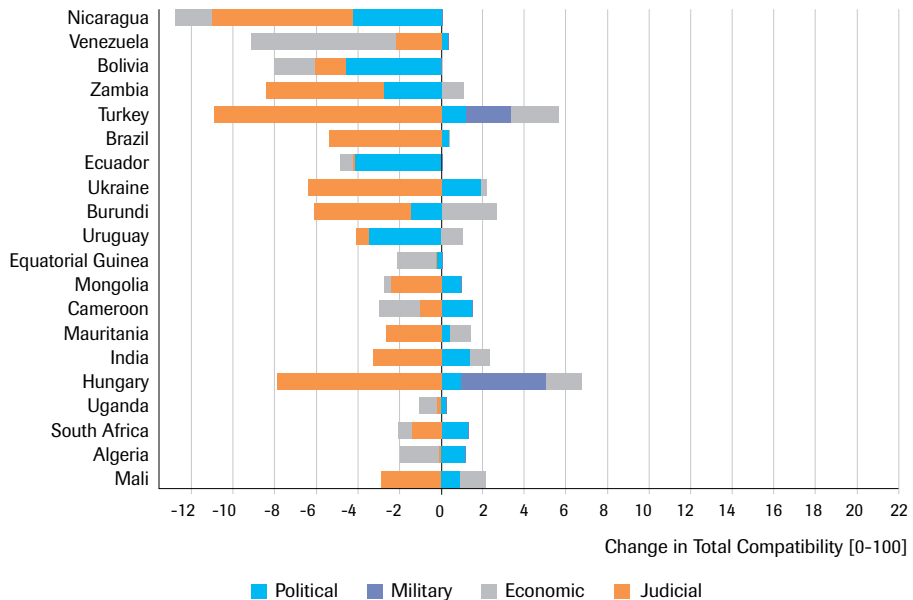


Figure 10 Top 20 largest decreases in total compatibility, broken down by domain



At the other end of the spectrum, we encounter well-known contradictors, such as Venezuela, which has gone through a process of even greater inimical alignment and economic deliberalization (see Figure 10). In general, many Latin American nations have become less similar to the Netherlands, indicating that several countries in this region have moved away from liberal political and economic values and from international political alignment.

Turkey and Hungary emerge as problematic allies. Economically they have moved closer to the Netherlands. These states have raised their military compatibility scores over time as measured by the DFRI through increased NATO and EU military cooperation, even if there are significant problems in these relationships as well, with Turkey positioning itself as an independent political and military actor in the context of the Middle East and the relationship with Russia. Judicially these states have gone through a process of democratic backsliding or even outright authoritarianism, leading to huge decreases in terms of judicial compatibility. These developments pose a clear problem for Dutch relations with these countries.

5.4 Sub-conclusions

In the context of the changing global distribution of power, Dutch relations with other states have changed quite substantially, along both the interests and the values spectra, as measured by the DFRI. The descriptive analysis of the DFRI offered in this chapter, which will be triangulated and corroborated with a review of secondary sources in next year's monitor, yields the following insights:

First and foremost, the Netherlands finds itself in a relatively fortunate position. It can count on close allies and partners in its immediate geographic surroundings. Moreover, the number of associates has increased considerably, while the number of contradictors has decreased, suggesting that there are more potential partners for the Netherlands while it faces fewer outright opponents.

Second, despite ongoing turbulence in the EU and the impact of Brexit, Europe is increasingly the most relevant region for the Netherlands. The US nevertheless remains the most important country in Dutch foreign relations, together with Germany. The US' position is undermined by the relative decline of its political and military influence in world politics. When taken collectively, the relevance of Europe dwarfs all competitors, stressing the vital importance of the EU internal market and its potential strength as a geopolitical bloc.

Third, China's stellar ascent economically, militarily, and politically, in combination with low compatibility in terms of shared values, underscores once again that China presents both an opportunity and a risk. China is across the board a force to be reckoned with in the design of future Dutch foreign policy.

Fourth, several states have increased in both relevance and compatibility. These prospects, such as Mexico, South Africa, and Israel, can be valuable partners for the Netherlands to collaborate with in shaping international regulation on important themes.

Finally, engaging with prospects and associate states that are becoming more relevant but that are moving away in terms of compatibility poses relevant dilemmas, which require careful assessment on a case-by-case – or state-by-state – basis. Especially judicially, a number of states are drifting away along the liberal democratic values spectrum. The balance between relevance and compatibility should always be taken into account in determining which relationships to invest in and from which to disengage. With states like Hungary and, to a lesser extent, Turkey, the strength of the existing relationship with the Netherlands is such that it can potentially be leveraged to reverse this process. The EU especially offers mechanisms to this end. With states that are less embedded in such partnerships, the compartmentalization of partnerships might be an option. If a state is (increasingly) far removed from the Netherlands along the judicial dimension, but closer in terms of economic similarity, partnerships focusing exclusively on economic affairs might be a possibility. Examples of such increasingly relevant autocratic states abound, with cases in point being the UAE and Saudi Arabia. The decision on whether to pragmatically engage with these countries is both politically and morally fraught with difficulties. Such compartmentalization, however, may be more difficult when it comes to the security domain. Overall, even if Dutch anchor states remain dominant in absolute terms, none experienced an increase in relative relevance in the past decade, while many prospect states increased remarkably. If the decline of Dutch traditional allies persists, the Netherlands may have to consider future 'coalitions of the willing', including countries that would as yet still be considered strange bedfellows.

6 Security is in the Eye of the Beholder

Decisions in international relations are shaped by the security and threat perceptions of the actors. These, in turn, are influenced by a range of factors: geography, history, culture, etc. Cognitive biases also play an important role in shaping these perceptions. Recognition of such biases can help decision-makers to establish a more balanced view of their environment and of the potential threats to national security.³¹⁷ This chapter first analyzes the role cognitive biases play in shaping security perceptions. It then examines how the six threat categories from chapter 2 are perceived in a set of 38 security documents published in other countries, what additional threats are identified in these documents, and how trends in the international order are evaluated, so as to identify potential 'gaps' in the Dutch security perceptions.

6.1 On the Role of Biases in Perceptions

Gaps between the reality of security and the human perception of it are not uncommon. This divergence is the result of intuitively made trade-offs. Humans are not very good at making security risk trade-offs. Daniel Kahneman, the Nobel Prize-winning psychologist, conducted research on people's estimates regarding the principal causes of death, after which he compared the results to statistics on the matter. One of the outcomes was that people thought hurricanes were bigger killers than asthma, even though asthma caused twenty times as many deaths as hurricanes did. This is only one of many examples that show that people's intuitive risk estimates are inadequate.

According to Schneier, several aspects of the security trade-off might be calculated wrongly: the severity of the risk, the probability of the risk, the magnitude of the costs, how effective a particular countermeasure is at mitigating the risk, and how well disparate risks and costs can be compared.³¹⁸ The more human perception deviates from reality in any of these aspects, the more the perceived trade-off deviates from the actual trade-off. These miscalculations have a lot to do with biases that are inherent in the human brain. Some of those biases and how they might affect our feeling of security are explained below. These biases can also partly explain the different perceptions countries

317 The paper *Perceptions of Security: How Our Brains Can Fool Us* is published on the Strategic Monitor website.

318 Bruce Schneier, "The Psychology of Security" (Springer-Verlag Berlin Heidelberg, 2008).

have with regard to security threats, as demonstrated by the comparative study in chapter 6. Because countries are led by people, and cognitive biases are inherent in the human brain, this naturally affects decisions that eventually evolve into national security policy and strategy.

6.1.1 Availability heuristic

One of the most common biases is the ‘availability heuristic’. Daniel Kahneman defines this as the process of judging frequency by “the ease with which instances come to mind.”³¹⁹ The biases that Kahneman describes give a good explanation for the discrepancy between actual and perceived security. It explains, for example, why people are more afraid to fly immediately after a plane crash occurred and why people get insurance right after major disasters. The examples remain vividly in people’s memories for some time. In addition, it can explain why people are disproportionately afraid of terrorist attacks (as compared to much more common ways to die): the examples are all over the news and frequently repeated. Consequently, people have a lot of examples fresh in their memories and therefore perceive the chance of terrorist attacks as much higher than it actually is.³²⁰ This bias also causes the overestimation of rare events: rare events attract a disproportionate level of attention, and the few instances that actually occur are all over the news. The regime type of states can be of central importance with respect to this bias. For example, in democracies, the existence of a free press, greater policy debates, institutional checks and balances, and the fact that more actors are involved in the decision-making process, raises the chances that particular tides of information can correct for cognitive biases.³²¹

6.1.2 Negativity bias vs. positivity bias

Another common bias of the human mind is known as the ‘negativity bias’. This negativity bias is seen as a fundamental principle of human cognition, in which negative factors have a greater impact than positive factors across a wide range of psychological phenomena.³²² Psychologists believe that the dominance of bad over good emerged as an adaptive trait to avoid lethal dangers in human evolutionary history.³²³ However, nowadays it could have some side effects that we should be aware of. For instance, this negativity bias could have an impact on the ‘threat sensitivity’ of states: how states

319 Daniel Kahneman, *Thinking, Fast and Slow*, 1st edition (New York: Farrar, Straus and Giroux, 2013).

320 E.E. Duchateau-Polkerman, “EMSD Thesis De Perceptie van Veiligheid” (Hogere Defensie Vorming, 2015).

321 Tierney Johnson, “Bad World: The Negativity Bias in International Politics,” *International Security* 43, no. 3 (2019).

322 Johnson.

323 R. F. Baumeister et al., “Bad Is Stronger than Good,” *Review of General Psychology* 5 (2001): 323–70; Johnson, “Bad World.”

identify opportunities and dangers prior to conflict. High threat sensitivity means a heightened reaction to negative information indicating potential dangers compared to positive information suggesting opportunities.³²⁴

A bias that at first glance seems to contradict the negativity bias is the 'positivity bias': overconfidence about own capacity, abilities, overestimating own control over events, over-optimism about future prospects.³²⁵ However, this bias could actually coexist with the negativity bias, because the biases apply to different contexts. People privilege negative information about the external environment and other actors, but positive information about themselves. The coexistence of these biases can raise the odds of conflict. Decision-makers simultaneously exaggerate the severity of threats and are overconfident about their own capacity to deal with the situation, a potential recipe for disaster.³²⁶

The effect of the negativity bias could be even stronger if it is combined with the so-called 'halo effect': the tendency to like (or dislike) everything about a person or situation (or country), including things you have not observed.³²⁷ We can see this kind of effect, for example, with regard to Russia: everything that Russia says or does nowadays is viewed from our negative perception of it. An act or statement that would be just fine or viewed neutrally if it came from Germany is viewed negatively and received with suspicion when it comes from Russia. The same halo effect, both positive and negative, can be observed with US President Trump. Most people, especially in America itself, either dislike everything he says or does or love it and will defend him no matter what. There seems to be little room for a balanced view in which positive, negative, and neutral statements can be judged on their merits.

6.1.3 Prospect theory vs. utility theory

Another common area in which the feeling of security is at odds with the reality is the perception of the severity of a certain risk. According to utility theory, which assumes that actors are fully rational and make trade-offs based on a calculation of relative gains and losses, people tend to choose alternatives with the same probability. However, the outcomes of experiments contradict the basic assumptions of utility theory. When faced with a gain, the majority of people prefer a sure gain over a risky gain. But when faced with a loss, the majority of people prefer a risky loss over a certain loss. This difference

324 Johnson, "Bad World."

325 Johnson.

326 Johnson.

327 Kahneman, *Thinking, Fast and Slow*.

can be explained by prospect theory, which, in contrast to utility theory, acknowledges that people have subjective values toward gains and losses.³²⁸

The fact that people act in this way can be attributed to the framing effect. As experiments show, people make different trade-offs when something is presented as a gain as opposed to a loss. The choices people make are affected by how the alternatives are framed. When a trade-off is framed in terms of a ‘gain’, people tend to be risk-averse, whereas when trade-offs are framed as a ‘loss’, people tend to be risk-seeking. This also applies to countries, because countries are led by people.³²⁹ Nowadays we see a trend whereby certain countries no longer view world economics or globalization as a win-win situation, but rather as a zero-sum game. Countries that see the world through a zero-sum game lens are likely to take more risk to avoid a bigger loss over what they view as a certain loss. America’s protectionist measures, for example, can partly be explained on this basis.

In conclusion, biases affect decisions that eventually evolve into a country’s national security policy and strategy. Policymakers should take the different perceptions of other countries into account, but also be aware of their own possible biases.

6.2 International Security Perceptions

Are we immune to biases in our own analyses and assessments? That would seem unlikely. The authors are not only human, but also Dutch and/or embedded in Dutch society and culture. We tend to build upon data and judgments from sources that are for the most part close to our ‘comfort zone’ (e.g., in terms of language, accessibility, and understanding based on cultural proximity). Because the Strategic Monitor aspires to inform the Netherlands’ foreign and security policy, we use existing structures from that policy as a reference. The clearest example of this is that the structure of chapter 0 reflects the six most urgent security threats from the Dutch *Integrated Foreign and Security Strategy 2018-2022*. In order to counterbalance some of these tendencies, we have looked at 38 individual documents sourced from eleven countries and six world-renowned think tanks and/or intergovernmental organizations (IGOs) (see Table 21).

328 Bruce Schneier, “The Psychology of Security,” 60.

329 Bruce Schneier, “The Psychology of Security.”

Table 21 List of the 38 documents sourced from countries, think tanks, and IGOs

Country	Publication (public)	Year	Think tank(s)	Publication (private)	Year
Australia	2016 Defence White Paper	2016	Australian Strategic Policy Institute	North of 26 degrees south and the security of Australia: views from The Strategist	2019
United States	Worldwide Threat Assessment	2019	US National Intelligence Council	Global Trends: Paradox of Progress	2017
China	China's National Defense in the New Era	2019	Institute of International and Strategic Studies, Peking University	Time and Tendency in the Changing World Situation	2019
Russia	Russian National Security Strategy	2015	Center for Strategic Research	Theses on Russia's Foreign Policy and Global Positioning (2017-2024)	2017
Israel	Israel Defense Forces Strategy Document	2015	Israel Defense	Israeli National Security: A New Strategy for an Era of Change	2018
India	Ministry of Defence: Annual Report 2017-2018	2018	Strategic Foresight Group	Big Questions of Our Time: The World Speaks	2016
Japan	Defense of Japan 2018	2018	The Japan Institute of International Affairs	A New Security Strategy for Addressing the Challenges in the Turbulent International Order	2018
Finland	Government's Defense Report	2017	The Finnish Institute of International Affairs	The Changing Global Order and its Implications for the EU	2019
Singapore	N/A	N/A	Centre for Strategic Futures	Foresight: 10th Anniversary Issue	2019
UAE	Future Outlook: 100 Trends for 2050	2017	The Emirates Centre for Strategic Studies and Research	United Arab Emirates Society in the Twenty-first Century: Issues and Challenges in a Changing World	2018
Peru	Peru 2030: Riesgos y Oportunidades	2019	Inter-American Dialogue	Why and How Latin America should think about the Future	2016

Institution	Publication	Year
Munich Security Conference	Munich Security Report 2019	2019
World Economic Forum	Global Risks Report 2019	2019
Zurich ETH	Strategic Trends 2019	2019
European Council on Foreign Relations	Strategic Sovereignty: Multiple Documents	2019
Center for Strategic and International Studies	Defense 2045	2015
ESPAS	Global Trends to 2030: Challenges and Choices for Europe	2019

Each country's security perspective was analyzed on the basis of two documents, one published by state institutions and one published by a local think tank. Each country's documents were analyzed on the basis of a standardized rubric which aimed to extract a longlist of identified threats – and countries' perceptions of those threats – in order to identify potential blind spots in the Dutch threat perception. The analysis allows not only for a comparative review of how the Dutch allies and adversaries perceive threats outlined in the Dutch *Integrated Foreign and Security Strategy 2018-2022* and in the Dutch *National Security Strategy* of 2019, but also for the identification of blind spots and opportunities. Think tank articles were analyzed largely with the goal of establishing each country's approach toward conducting strategic foresight. The objective of the exercise was to answer the following research questions:

1. How do these assessments appraise the six threat themes central in Dutch strategy?
2. What additional threats ('gaps' for the Dutch) are identified in these assessments?
3. How do these assessments evaluate the international order?
4. Do these studies reflect on opportunities?

The next sections address these questions.

6.2.1 Perceptions of the six threat themes

First, the threat of military confrontation is identified by Finland, India, Israel, Japan, Russia, the US, and China. The European Strategy and Policy Analysis System (ESPAS) and the Munich Security Conference (MSC) additionally pay lip service to the notion of a growing threat of an eruption of interstate armed conflict. Among all these actors, the most commonly held view – shared by the Netherlands – manifests itself in the perception that an increase in interstate competition increases the risk of a military competition. China, the US, Japan, and Russia place emphasis on their competitors' efforts at military modernization, pointing to increasing defense budgets and the unveiling of cutting-edge (conventional) weapons systems as signs of aggression. India, Israel, and Japan all view interstate competition through the lens of either a) the regional dynamics on which it is based, or b) the regional insecurity it is likely to exacerbate, thus

departing from the Dutch perspective. Outside of the ESPAS and the MSC, no think tanks share (or explicitly formulate) the Dutch view that the international legal order faces erosion.

Second, the UAE, Singapore, Finland, Japan, Israel, the US, and Australia explicitly elaborate on the threats posed by malicious actors' activities in cyberspace, as do the ESPAS, the MSC, the Center for Strategic and International Studies (CSIS), and the World Economic Forum (WEF). The UAE, Finland, Japan, the CSIS, the WEF, Israel, the US, and Australia all emphasize systems' interdependencies in critical infrastructure as a factor serving to heighten their societies' vulnerability to cyberattacks. In further alignment with the Netherlands, the UAE, Japan, the WEF, Israel, and the US subscribe to the notion that the cyber domain's penetration of virtually all spheres of life creates further vulnerabilities and/or vectors for cyberattacks. The sentiment that cyber- and/or IT-related innovations are likely to upset existing power dynamics (whether military or otherwise) constitutes a marked departure from the Dutch view on cyber threats. Whereas the Netherlands perceives cyber threats almost exclusively through the lens of cyberattacks (i.e., the threatening use case), several actors – the UAE, the ESPAS, Japan, the CSIS, and the WEF – view the cyber domain as one which is likely to form the backdrop of a new wave of interstate competition.

Third, the vast majority of countries that identify hybrid conflict and/or gray zone operations as a threat at least pay lip service to the phenomenon of unwanted foreign influences, and discuss these also in relation to economic security. Finland, the US, Japan, the UAE, the ESPAS, the CSIS, and the European Council on Foreign Relations (ECFR) all touch upon influence campaigns as a threat. Common within this subset of countries is a focus on a) new technologies, and b) vulnerabilities brought about by societal openness – both factors which the Netherlands outlines explicitly. The Dutch perception that hybrid tactics increasingly take the form of – and infringe upon – the country's vital economic processes is only sparsely shared. Finland identifies the disruption of critical supply chains as a threat deriving from the increasing assertiveness of its Russian neighbor, but focuses most prominently on energy-related supply chains. India and the UAE pay lip service to the notion that cyber tools play a role in unwanted technology transfers, but do not explicitly tie the phenomenon to hybrid conflict. Another clear divergence manifests itself in the intended use of hybrid tactics as an offensive tool. European countries and entities (the Netherlands, Finland, the ESPAS, and the ECFR) perceive the offensive use of hybrid tactics as reflecting not only an increase in great power competition, but also a concentrated effort on behalf of perpetrating actors to erode their societies' ability to react to foreign developments. The US, China, and Russia universally perceive the offensive use of hybrid threats as being geared predominantly toward fostering influence internationally, as well as being geared toward inflicting physical and/or economic damage on the domestic front.

Fourth, CBRN weapons are explicitly identified as a threat by India, Israel, Japan, the US, and the UAE. Within this country sample, three of the Dutch observations regarding the threat posed by CBRN weapons are widely shared, namely a) interstate competition's role in incentivizing a so-called race to the bottom, b) the likely destabilizing impact of technological developments, and c) the threats posed by non-state actors. Whereas, as it relates to interstate competition, the theme surrounding technological developments centers almost entirely around nuclear weapons, its interaction with the threat posed by non-state actors derives from the access to CBRN weapons these developments are likely to give them. The Japanese and UAE perspectives are preoccupied most prominently with chemical and biological weapons, contending that new technologies and access to information and/or blueprints over the Internet have significantly reduced the threshold of access for non-state actors.

Finally, Dutch perceptions regarding terrorism are widely shared by the countries included in this study. Singapore, India, Finland, Japan, the UAE, Israel, the US, Russia, Australia, and China identify – and give a central position to – terrorism within their national security strategies. In a marked departure from the Dutch perspective, India, the UAE, Israel, the US, Russia, and China identify terrorism as a phenomenon which is (at least partially) dependent on – and derives from – state support, thus politicizing it as an issue and overtly linking it to hybrid warfare and foreign interference. While the Netherlands identifies right-wing extremism as being generally less impactful than its Islamist counterpart, the ESPAS, the MSC and the US present right-wing extremism as posing a threat that equals (or even surpasses) the threat posed by Islamic extremism.

6.2.2 What additional security threats are identified?

The threats identified by the Netherlands, topical and/or relevant as they are, do not constitute a comprehensive list. Our report identifies a total of 31 distinct threats, which have been sorted into eight clusters to facilitate further analysis (see Table 22).

Table 22 Longlist of identified categories and threats

Categories	Threats
Technology-related	Biotechnology – Space militarization – Technological innovation – Military technological innovation
Gray zone operations	Cyber domain – Counterintelligence – Economic coercion – Hybrid warfare – Influence operations – Proxies – Energy security
Climate risks	Climate change - Energy production & consumption - Environmental threats
Human security & development	Demographics - Human security - Large-scale migration - Public health - Urbanization

Categories	Threats
Societal & national identity	Quality of Life - National Identity & Societal Threats
International instability	Great Power Politics - International Instability - Inter & Intra State Conflict - Regional Instability - WMD Proliferation
Violent non-state actors	Public Order - International Criminal Organizations - Terrorism
Economic & financial	Trade System - Economic and Financial Stability

Dutch threat perceptions are largely represented in the ‘violent non-state actors’, ‘economic & financial’, ‘gray zone operations’, ‘international instability’, and, to a lesser degree, ‘technology-related’ threat clusters. This means that ‘climate risks’, ‘human security & development’, and ‘social and national identity’ constitute threat clusters which are underrepresented within the Dutch threat perception framework.

Zooming in on specific threats, several threats – even within the previously outlined threat clusters – do not recur clearly in the Dutch threat perception. Biotechnologies are touched upon within the context of terrorist threats, but not within the context of state competition. Space militarization is not explicitly mentioned. Neither proxies nor energy security are explicitly referred to in the context of the Dutch understanding of hybrid threats. Large-scale migration is touched upon as a threat to Dutch domestic stability, but is not tied to (contributing) threats such as those outlined under the ‘climate risks’, ‘human security & development’, and ‘societal and national identity’ threat clusters. In concrete terms, this means that biotechnologies, space militarization, state use of proxies, energy security (through a hybrid lens), climate change, energy production & consumption, environmental threats, demographics, urbanization, and national identity & societal crises constitute threats which may warrant incorporation into the Dutch threat perception framework.

First, biosecurity is identified as a threat by the CSIS, Japan, Russia, Singapore, the US, the WEF, and ETH Zurich. These actors posit that advancements in the field of synthetic biology will allow the design and construction of new “biological parts, devices, and systems and the re-design of existing, natural biological systems for useful purposes.” Explicit links are made to a heightening of the threat posed by CBRN weapons, which is correlated most directly with terrorist threats. Dual-use technologies (i.e., CRISPR) are singled out as drivers of the increased (perceived) threat level.

Second, militarization of space is identified as a threat by Australia, China, Finland, India, and Japan. These systems are viewed as offering advanced surveillance opportunities and are generally expected to become of relevance within the next twenty years.

Third, energy security and energy consumption and production are identified as threat categories by Finland, India, Russia, and the UAE. Energy security is typically quoted as a threat which derives from identifying countries' high degree of dependence on other countries or on international supply chains, meaning that the threat's identification is endemically tied to the fear of a disruption. Energy security is also viewed as being negatively impacted by radicalization (India). The most commonly cited 'solution' to this threat manifests itself in a reduction of domestic energy consumption.

Fourth, climate change and environmental threats are identified as threat categories by Australia, the CSIS, the ESPAS, the ECFR, Finland, India, Japan, Peru, Russia, the UAE, the US, the WEF, and ETH Zurich. Climate change is generally understood as a threat which contributes to migration flows and/or to an increase in the initiation rate of intrastate conflicts. It is also linked to threats to physical and economic safety (see wildfires, flash floods, loss of biodiversity, etc.), as well as to political polarization. Environmental threats tie into climate change and are most commonly associated with food shortages and ecosystem failure. The disruption of supply chains is also tied explicitly to negative impacts on human security and quality of life.

Fifth, demographics are identified as a threat by Australia, the CSIS, China, the ESPAS, India, Peru, Russia, Singapore, the UAE, the WEF, and ETH Zurich. Demographics constitute a complicated threat category, often tied to urbanization and to interstate competition. Particularly when combined with a sizable young population and a relatively low level of development, urbanization as a phenomenon is tied by several countries to the initiation of intrastate conflicts, in no small part because a low level of development is associated with countries' failure to provide the public services necessary to secure an adequate quality of life in urban environments. Demographic growth is also identified by several countries as a driver of competitors' activities in the international arena.

Finally, identity and social crises are identified as a threat by the CSIS, Singapore, the UAE, Russia, and the WEF. These crises are generally described as deriving from ethnic, religious, and/or political fault lines in society, and are associated with (among others) an increase in the risk posed by terrorism and heightened vulnerability to misinformation campaigns.

6.2.3 How is the state of the international order evaluated?

The assessments included in this study identify the intensification of interstate competition and technological developments as key factors shaping the international order. Although the international order is universally identified as eroding, perceptions regarding its nature are split between 'status quo', 'anti-status quo', and

'bystander' descriptions of the order. Status quo descriptions – offered by assessments published in Australia, Finland, Japan, Peru, the US, and the Netherlands – universally perceive the maintenance of the rules-based international order as a priority. They identify the combination of interstate competition within the military, economic, and diplomatic domains, combined with the erosion of international adherence to democracy, as undermining it. Anti-status quo assessments, as published in China and Russia, also posit that the existing international order has come under siege as a result of interstate competition, but they point to the US' infringements of international agreements as evidence of its continuing decline. Finally, bystander assessments such as those from India, the UAE, and – to a lesser degree – Singapore, outline the notion that an international power shift toward the Asia-Pacific region will require the forging of new partnerships in the near future, a sentiment shared by China and Russia.

Aside from the effects of international competition, several actors identify new technologies as driving a paradigm shift in the nature of the international system. Most prominently, assessments from India, Japan, Peru, the US, and the UAE identify the dangers current technologies pose to democracy, the role they play in eroding support for the rules-based order among its most committed defenders, as well as in empowering malicious non-state actors to overcome asymmetries in conventional capabilities and to operate outside the bounds of the rules-based international order. Also of relevance is the emphasis on the advent of new technologies, the inequality of their distribution, and their concentration within private-sector actors, which is likely to result in a diffusion of power away from states and in the emergence of entirely new governance models.

6.2.4 Opportunities

The analysis of the documents revealed an overwhelming focus on threats. Nonetheless, a number of opportunities were also posited. Most of these could be qualified as 'silver linings in the clouds': overall negative developments that can also possibly trigger positive outcomes. Multiple assessments argue that various existential crises (e.g., rampant Euroscepticism, climate change, great power competition, etc.) offer room for the radical restructuring of existing institutions and/or interstate relations. In the face of eroding global institutional regimes, attention is drawn to the ability of regional institutions to address international problems. In addition, many assessments emphasize that the disruptive effects of new technologies can at least be partially offset by the potential opportunities they can engender, observing that they will boost economic growth, facilitate the development of increasingly robust public services, and contribute to the mitigation of negative externalities associated with income inequality.

6.3 Sub-conclusions

The analysis offered in this chapter warrants three important overarching conclusions. First, awareness of cognitive biases that shape our security perceptions is of vital importance for a balanced view of our security environment. Second, a number of international security documents not only appraise the threats prevalent in Dutch security and foreign policy discourse differently, but also give greater weight to additional threats, including the impacts of climate change and the exploitation and militarization of space. Third, most of these documents pay very little attention to the other side of the security coin: opportunities.³³⁰ In our view, it therefore merits recommendation to take all three of these conclusions into consideration in the design of next year's strategic anticipation activities in the framework of the Strategic Monitor. Moreover, we suggest also including the results of a survey conducted among the Dutch population regarding our own, national security perceptions (the Clingendael Barometer).

330 Stephan De Spiegeleire and Tim Sweijs, "The Other Side of the Security Coin," HCSS, 2017.

7 Conclusion

The tenets of the international order continue to shift. The worldviews of the major global powers conflict, their value systems diverge, and their incentive structures are misaligned. The result is an intensification of interstate competition in recent years. Verbal assertiveness, with threats being part and parcel of diplomatic discourse, is complemented by actual assertive behavior in important areas of international relations. States openly contest the terms of international trade and are actively jockeying to reap the fruits of the algorithmic revolution. Their competition over protocols and standards for next-generation technologies is both about the protection of national security and about economic dominance over the nascent fourth industrial revolution. It is also emblematic of the stakes involved in the rivalry between the US and China – with Europe largely sidelined – over technological supremacy, in which political, economic, and national security considerations are increasingly intertwined.

This increased global competition goes hand in hand with a persistent erosion of significant aspects of the existing architecture of the international order, ranging from the demise of arms control regimes, such as the INF Treaty, to the hamstringing of the WTO's court of appeal by the US, as a key component of the liberal trading order. While many of the day-to-day discussions put the onus on US President Trump, it is clear that the erosion stems from more structural developments. The US withdrawal from the INF Treaty takes place against the backdrop of a multipolar world and the limited scope of the Treaty, excluding China with its growing arsenal of medium-range missiles. In a similar vein, 'America First' is not the cause but a tell-tale symptom of the erosion of the liberal trading order. The underlying trend concerns the effects of hyper globalization on domestic distributions of income and wealth in the West from the 1980s onwards in the context of declining competitiveness of labor-intensive industrial sectors. These deleterious effects in turn eroded the domestic base that undergirded the support for the liberal market order, not only in the US but in Europe as well.³³¹

It is important to recognize that it is the combination of national and international vectors that converge to undermine various bastions of the existing international order, both from within and from without, both bottom-up and top-down. Our analysis of global geodynamics yields a kaleidoscopic picture. The world population has become more prosperous, but inequality has also increased by different measures. Although

331 Jonathan Hopkin and Mark Blyth, "The Global Economics of European Populism: Growth Regimes and Party System Change in Europe," *Government and Opposition* 54, no. 2 (April 2015): 193–225.

the world as a whole continues to become more connected, increased connectivity has not necessarily brought people closer together. Societies worldwide have not become more inclusionary, due to a marked increase in identity-driven politics, higher levels of religious restrictiveness, and increases in social hostilities. At the same time, the rule of law has been strengthened and, despite the structural human rights violations in a number of countries, human rights protection regimes are improving over time. But despite the growth and spread of democracy over the past two decades, democracy as an institution and especially individual freedoms are under prolonged attack. Civil and political rights have been declining for over a decade now, in both free and unfree countries. At the same time, illiberal governments have undeniably been gaining more influence in the regulation of global affairs. Finally, over the past two decades, the world has become less peaceful and secure because of a growing number of conflicts and conflict fatalities.

At the same time, illiberal governments have undeniably been gaining more influence in the regulation of global affairs. Their waxing influence derives from stronger involvement in existing institutions (e.g., China in the United Nations Security Council), from the establishment of new institutions and initiatives (e.g., China and the Asian Development Infrastructure Investment Bank and the Belt and Road Initiative), and from a much more proactive diplomacy based on a larger foreign military footprint than before (e.g., Russia, Turkey, and Iran in the Middle East and beyond). This coincides with the US vacillating between engagement and disengagement, to the detriment of longstanding partnerships in various regions, including the Middle East and Europe.

In this context, compliance and cooperation are giving way to violation and confrontation across important political, economic, and security regimes. Rules are systematically violated, while underlying norms are incrementally hollowed out. This shift is consistent with observations in previous editions of the Strategic Monitor, but is now even more pronounced. The factors driving these developments, both at the national and the international level, are structural in nature, and are not likely to suddenly lose strength or change direction any time soon. A further erosion and adaptation of the regimes underpinning the order should be expected. The outlook for the international order is therefore that this macro-trend is not likely to change in the next few years.

Despite this negative outlook, it is equally important to note that there are certainly areas in which international cooperation persists, albeit more often in the context of voluntary and non-binding initiatives of coalitions of the able and the willing, comprised of national and local governments, and increasingly in partnership with non-state actors. Such coalitions take on transnational challenges, ranging from addressing the effects of climate change to designing regulations to deal with cyber risks. The Paris Call for Trust and Security in Cyberspace received support from a mixed coalition, including 75 states, 26 public authorities and local governments, 340 international and civil society

organizations, and 624 corporations.³³² It epitomizes another aspect of the global redistribution of power alongside the geographical reorientation, namely power diffusion from states to various types of non-state actors.

These shifts all take place in an era of rapid technological change. The past few years have seen considerable advances both in computing (processing) power and in algorithms that are progressively being integrated in and implemented across a wide range of industries. Although Moore's Law combined with advances in machine learning does not translate into exponential rates of change in the real world, it is undeniably driving the pace of economic, political, societal, and military processes. Rapid technological development offers opportunities to make the world a better place, among others by enhancing food production, finding better cures for diseases, and in time perhaps even reducing our ecological footprint.³³³

But it also generates a whole host of new challenges to political and societal cohesion, economic equality, national security, and fundamental human rights. These present policymakers with important questions such as: how to deal with digital divides, winner-takes-all dynamics, and concomitant growing wedges in income and wealth; how to address comprehensive forms of data collection by public but also private actors and how to protect privacy; how to shield democratic discourses from being manipulated for commercial or political gain; and how to ensure the integrity and security of critical infrastructures in the context of globally integrated vendor and supply chain markets. The headlines of 2019 are indicative of a range of important challenges that our polities are starting to grapple with in a new context.

These challenges also manifest themselves in the trends and developments analyzed within the six main threat themes. Our multi-component assessment of the threats associated with military competition, cyber security, hybrid conflict, economic security, CBRN weapons, and the nexus between terrorism and technology paints a predominantly negative picture. Here too there is an alignment of various vectors that amplify threats across these themes. The intentions, capabilities, and activities of the principal actors clearly point to a deterioration of the security environment. Increasing interstate competition over power, security, and prosperity features considerable strategic experimentation and innovation, both in traditional military and economic domains and in the cyber domain. Opportunities offered by technological advances are actively sought and exploited. Resurgent and emerging powers increasingly deploy hybrid tactics targeting both virtual and physical assets. Even if their purpose is to gain incremental advantages while staying below the threshold of war, the risk of escalation

332 "Paris Call for Trust and Security in Cyberspace – Paris Call," accessed December 9, 2019.

333 Peter Diamandis, "Abundance: The Future Is Better Than You Think," 2013.

is real. Some authors have observed that major war is far from obsolete, whereas others assert that it is “less unlikely.”³³⁴

But even absent escalation, interstate competition is having important implications for the nature of threats, the vulnerability of our societies to contemporary threats, and the type of reaction this is engendering among state actors. Conceptually speaking, these implications involve the further fusion of the internal-external security nexus, with the global affecting the local and vice versa. Borders, physical or otherwise, do not shield against the dangers posed by external forces. This leads to what military strategists refer to as strategic compression, or the compression of time and geographical distance. Threat actors can act over longer distances in shorter amounts of time. It also implies the spillover of threats from one domain to another, with multidomain threats becoming the rule rather than the exception. In addressing these contemporary threats, national governments are assuming more responsibilities and expanding their roles. They do so by trying to augment their reach and extend their control. Various states are bringing critical infrastructures, including the Internet, under national control, while they re-evaluate the use of global manufacturing supply chains for critical technologies. This can be expected to put a dent in globalization and is likely to affect the shape of economic and security regimes that will be part of the emerging order. States are also building in multidomain capabilities, further developing and refining whole-of-government approaches, both on the defensive and on the offensive side. With the nature of the security environment evolving, state exploration of new concepts and strategies concerning how to address threats and harness opportunities has only just begun. As these exploratory efforts gain more flesh and substance in the years to come, they will be important factors in shaping the rules of the international order.

Do the developments described here signify the full demise of the existing international order, or do they merely represent a perhaps overdue renovation of regimes within that order that are no longer fit for purpose? We would argue that the developments suggest a little bit of both: some elements in the existing international order are revised and brought in sync with the global distribution of power; other elements are redesigned from scratch. This leaves the shape of the emerging international order still uncertain but not entirely unclear. Based on our analysis, on our reading of the writing on the wall, the following observations pertaining to the international order over the next five years seem justified.

First, interstate relations are likely to feature more outright forms of competition in the economic, military, but also the ideological realm. Expect more explicit expressions of self-interest to be accompanied by more explicit policies directed at asserting self-

334 Bear F. Braumoeller, *Only the Dead: The Persistence of War in the Modern Age* (Oxford University Press, 2019).

interest. Note that interstate competition does not preclude interstate cooperation, nor does it necessarily imply interstate conflict.

For the dominant power, the US, that competition straddles all domains but begins and ends with military competition, a way of thinking largely alien to European leaders and populations. A still dominant stream in US thinking propagates military preeminence, which envisions the US being able to militarily dominate any other power, including China. This is more than mere Beltway talk. Official strategies have been formulated and budgets allocated in support of that goal, and the Pentagon is gearing up for long-term rivalry with China. Europe does not really feature in that vision, other than that it should be able to defend itself against Russia in a conflict in the European theater, freeing up American resources to fight and win in the Indo-Pacific theater.

Expect, alongside a strategy of military preeminence, elements of economic retrenchment and protectionism to become part of US policies. Declining levels of competitiveness of traditional industries and greater competition in emerging industries are likely to lead the US to implement more protectionist policies irrespective of the occupant of the White House. The nature as well as the extent of that retrenchment is uncertain. It may transpire gradually and in a consultative and collaborative way within a multilateral framework, or it may follow a more abrupt, assertive, and unilateralist course as pursued by the current administration. How this will eventually play out also depends on the responses of the two other economic powerhouses, China and the EU, but expect these latter two actors not to sit idly by. Confronted with US protectionism, they are likely to pursue reciprocal strategies.

The dynamics of US-Sino rivalry will be different from those between the US and the Soviet Union in the Cold War and will take place across multiple domains. In the Cold War, the principal competition was between two blocs of states with very little economic interlinkages between them. Many states in the periphery were left largely on the sidelines in terms of economic and political integration within these blocs. The current system is characterized by vastly deeper economic integration not just in terms of bilateral trade but also in terms of integrated global supply chain networks and foreign direct investment both between the two most important powers, China and the US, and between a larger number of states and groups of states such as the EU in that system. Interdependence can contribute to stability by creating mutual interests, but it can also contribute to spillover effects which fuel negative spiral dynamics. Expect state actors to actively pursue issue linkage strategies which will force others to confront real trade-offs between colliding interests. Two dangers that lurk are first, in the economic domain, the widespread implementation of beggar-thy-neighbor policies which will drive an economic race to the bottom; and second, economic uncoupling into different blocs around the US and China, which will remove incentives to constrain competition in other domains, most importantly the military domain.

Out of the current context, expect for the foreseeable future looser alliances in the context of an overall looser hierarchy within the system. The Cold War was characterized by a bipolar hierarchy with clear leadership, relatively tight alliance systems, especially in the core, and clear avenues for coordination within and between these blocs. In the emerging system, some alliance relationships may tighten (for instance the Japan-US alliance), but a more general trend points toward to the loosening of alliance relations, understood both in a formal sense (e.g., US and Turkey vis-à-vis NATO, for instance) and in a more informal sense, with states not wanting to be forced into one bloc or another. Singapore's Prime Minister Lee Hsien Loong's public demand not to be "pressured to take sides" at the Shangri-La Dialogue in June 2019 exemplifies the latter.³³⁵ Looseness of alliances can be a source of instability because of the uncertainty and unpredictability it injects into the order, but if it prevents the polarization of the states in the system in two blocs along rigid ideological lines with no cross-cutting cleavages, it can act as a strongly stabilizing force.

On the ideological front, expect increasing recognition of the fact that liberal democratic states and illiberal states have different value systems. It will become accepted that these differences cannot be ignored, condemned, or wished away, as used to be the dominant response especially in the West. Recognition implies neither moral justification nor acceptance, but stems from acknowledging that these value systems are different and must be dealt with. This recognition results from two factors. First, the majority of the generation of current political leadership in the West, having had multiple wake-up calls, are now more or less accustomed to the 'new normal'. Putting this differently, the notion has been brought home that other leaders really see things differently and are not likely to come around to a Western way of thinking. Second, parts of Western populations are not as dismissive of such value systems as the majorities in their societies are, meaning that illiberal world views are not dismissed right off the bat and will receive an audience through globally operating traditional and modern (social) media, and therefore be part of societal discourses.

What does this mean for the international order, or the collection of regimes that together constitute the international order? Our projection is that the reinvigoration of the liberal order, under renewed leadership of the US, is not likely to take place. A change in leadership in the US (and whether US policies will be characterized by restraint, retrenchment, or collaboration) will certainly have an impact on the liberal scope of the international order.³³⁶ However, the structural nature of international and domestic developments described in this study is likely to drive the international order's

335 "Singapore PM Tells China and US Not to Force Small Nations to Take Sides," South China Morning Post, June 1, 2019.

336 As a variation on existing taxonomies. This one is inspired by Hans Binnendijk, "Friends, Foes, and Future Directions: U.S. Partnerships in a Turbulent World: Strategic Rethink," Product Page, 2016.

further adaptation in line with new concerns and demands by leading protagonists. The order is therefore likely to become less liberal in nature and less global in scope, as it will be more fragmented. To some degree, the international liberal order will therefore become thinner in breadth and scope, certainly compared to the expectations and aspirations of political thinkers and leaders of the 1990s and the 2000s.

The types of coordination arrangements between states that are likely to become dominant are as yet uncertain. At this stage, it is too early to say whether a contemporary Concert of Great Powers will emerge as the centrally coordinating mechanism, similar to the post-1815 period on the European continent, or whether changing, ad hoc constellations of great and middle powers – depending on the issue area – will be more salient. Meanwhile, the formation of new international organizations and the refurbishment of existing ones that will come to play a role in coordinating mechanisms is a possibility.

Two countervailing forces are nevertheless worth considering. First, the international order as such is starting from a much higher baseline compared to previous eras when orders became dislodged, for instance in the 1910s and 1930s. There is a much thicker patchwork of treaties and agreements covering a vastly broader spectrum of activities and involving a much more diverse array of participants, both in terms of the number of states and in terms of the number of private actors. Modern means of communication and transportation will continue to facilitate coordination and collaboration that underpin the regimes that make up the order. Vested (establishment) interests, both public and private, will continue to argue for international coordination and collaboration. So even if the liberal nature of aspects of the order diminish, international regulation coordinated between states that have assumed greater roles in the regulation of their societies than in the past is expected to persist across a range of international dossiers over the next few years.

Second, despite ideological differences and competing interests, the pressure to act on various key international dossiers – e.g., climate change or nuclear weapon proliferation – may become so intense that global political leaders will see themselves forced to act. Enabled by technological means and spurred on by their citizens and responsible corporations, the urgency of the challenges may help them overcome the problems typically associated with collective action. Granted, it is not certain that this will in fact happen, but especially if confronted with the immediately visible impact of such challenges it would not be the first time that political leaders manage to figure out solutions that serve the common global good.

What does this outlook mean for the Netherlands? Policy recommendations fall outside the scope of the Strategic Monitor, but a few observations are in order to bridge the

gap between the high-level findings uncovered in research exercises such as this and insights that are more directly actionable for policymakers, at least those that are tasked with longer-term and strategic foreign and security policymaking.

Our high-level analysis of the Dutch position vis-à-vis other countries based on the DFRI suggests first and foremost that the Netherlands finds itself in a fortuitous position, with an assortment of close allies and partners in geographic proximity that are tightly integrated in joint economic, political, and security coordination arrangements. In terms of values, many countries have moved closer to the Netherlands, indicating that the Netherlands faces fewer outright opponents and more potential partners. Despite ongoing turbulence in the EU, Europe continues to grow in relevance. The US remains the most important country, although it has become less important in relative terms, with Germany as a close second. While these countries continue to be dominant in Dutch foreign relations, emerging powers have become increasingly relevant as measured along economic, political, and military dimensions over the past ten years. This is a sign of the changing international context in which the Netherlands operates. Especially China's rapid economic, military, and political ascent, combined with the fact that it is not aligned with Dutch core values, highlights that China presents opportunities as well as risks in the design of future Dutch foreign policies. In addition, a number of middle powers have increased both in relevance and in compatibility, which means that the Netherlands has a range of potential partners to collaborate with in shaping international regimes and regulations in this changing context.

In light of increasing competition in the context of a decaying order, lopsided dependence on single actors across multiple fields is potentially dangerous. This is the case in a direct sense, because it reduces the Netherlands' room for maneuver due to risks associated with issue linkage, but also in a more indirect sense, because it leads to polarization, not just within blocs but also across blocs, which in turn is not conducive to stability in the overall system. Put in more concrete terms, military dependency on an increasingly protectionist US may mean that the Netherlands sees itself forced to make economic choices that are not in its direct interest. If that happens repeatedly, it will contribute to the polarization of blocs, not just in the economic but also in the military domain, in a global context. Investing in greater strategic autonomy, not just militarily but also economically and politically, creates greater maneuvering room, which in turn contributes not only to the security and prosperity of the Netherlands but also to the stability of the system at large.

The growing relevance of European countries, and the regulatory power of the European Union across important economic and sociopolitical domains, means that strong collaboration within Europe will be indispensable. This should be approached certainly not as an end in itself, but rather as an instrument that can be used to protect Dutch

interests. At the same time, the changing context and the adaptation of the existing order require greater investment in bilateral relationships to build and strengthen partnerships that can help achieve Dutch core interests, both inside and outside of multilateral frameworks.

In selecting partnerships and making strategic choices, it is vital to have a clear understanding both of the vulnerabilities to which the Netherlands is exposed and the opportunities the Netherlands can leverage. How these interests can be served in a world that is closely integrated along many different dimensions is neither trivial nor simple. Deliberations and decisions concerning such choices should not only be reached on the basis of qualitative argument, but should be informed by granular and where possible empirical assessments. Cost and benefit assessments should take into account not just direct but also indirect effects. Whereas these types of assessments are fairly mainstream in general Dutch policymaking, with the research of statistical agencies playing a central role in decision-making on important policy matters, there is ample opportunity for improvement in this realm.³³⁷ ‘The empirical turn’ in foreign and security policy decision-making should still be firmly guided by normative convictions but should exploit level-headed assessments of how policies affect Dutch interests.

The changing context not only requires new partnerships based on such assessments, but also requires concept development and experimentation with new policy concepts to keep up with the evolving foreign policy environment. The pioneering of flow security concepts and connectivity strategies are two visible examples of some of the initiatives that Western public actors have been cautiously developing in this respect, but in a changing context concept development and experimentation deserves much greater priority than it is currently given.

Finally, the changing international context does not mean that we should ignore or under-appreciate our own values. It rather means the opposite. Increasing rivalry between values systems in the world requires that we also make more explicit what we stand for, and which way of life we want to protect and develop, and that where possible we actively use our values as an instrument of power and influence.

337 Although there are certainly positive exceptions here, see for instance, “De Nederlandse Importafhankelijkheid van China, Rusland En de VS” (Centraal Bureau voor de Statistiek, November 2019).

8 Bibliography

- “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter).” United Nations, 2009 2008.
- “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter).” United Nations, 2011 2010.
- “Actions with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression (Chapter VII of the Charter).” United Nations, 2013 2012.
- Acton, James M. “Why Is Nuclear Entanglement So Dangerous?” Carnegie Endowment for International Peace, January 2019.
- Adája Stoetman, and Minke Meijnders. “Economic Security with Chinese Characteristics.” Clingendael, November 2019.
- Adnan, Isabel Coles and Ghassan. “Iraq, Rocked by Protests, Enters New Phase of Uncertainty After Premier’s Resignation.” *Wall Street Journal*, December 1, 2019, sec. World.
- Agencies. “Spanish Police Clash with Thousands of Catalan Protesters in Barcelona.” *The Guardian*, October 27, 2019, sec. World news.
- Aileen Murphy. “The Trump Administration Is Eager to Sell Nuclear Reactors to Saudi Arabia. But Why?” *Bulletin of the Atomic Scientists* (blog), April 16, 2019.
- “AIVD Annual Report 2018 - Annual Report,” May 14, 2019.
- Alexander Klimburg. “Cybercriminals as Extensions of State Power?” ISPI, July 2018.
- Alexandra S. Levine. “Facebook, Twitter and Google Testify on Extremism.” *POLITICO*, September 18, 2019.
- Alice Poidevin. “What Does the Future Hold for US Trade Policy?” *European Centre for International Political Economy* (blog), February 2019.
- Alicia Sanders-Zakre, and Daryl Kimball. “Responses to Violations of the Norm Against Chemical Weapons.” *Arms Control Association* (blog), April 2019.

- Alvaredo, Facundo, Lucas Chancel, Thomas Piketty, Emmanuel Saez, and Gabriel Zucman. *World Inequality Report 2018*. Harvard University Press, 2018.
- Álvarez Ortega, Elena-Laura. “The Attribution of International Responsibility to a State for Conduct of Private Individuals within the Territory of Another State (La Atribución De Responsabilidad Internacional a Un Estado Por La Conducta De Particulares En El Territorio De Otro Estado).” SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, January 1, 2015.
- Amrita Khalid. “Anti-Extremism Group Run by Social Media Giants Becomes Independent.” *Engadget*, September 23, 2019.
- Tech Against Terrorism. “Analysis: The Use of Open-Source Software by Terrorists and Violent Extremists,” 2019.
- Arbatov, Alexey. “Mad Momentum Redux? The Rise and Fall of Nuclear Arms Control.” *Survival* 61, no. 3 (May 4, 2019): 7–38.
- “Artificial Intelligence: Expert Committee to Explore the Development of a Legal Framework,” September 2019.
- Ashley Roque. “USSTRATCOM Commander Paints Dour Future for New START.” *Jane’s 360* (blog), February 2019.
- Associated Press. “Donald Trump Threatens ‘Total Destruction’ of North Korea over Nuclear Programme during UN Address.” *South China Morning Post*, September 19, 2017.
- Astrasheuskaya, Nastassia. “Russia Gives Nuclear Group Control of Arctic Sea Route.” *Financial Times*, December 13, 2018.
- Bailey, Michael A., Anton Strezhnev, and Erik Voeten. “Estimating Dynamic State Preferences from United Nations Voting Data.” *Journal of Conflict Resolution* 61, no. 2 (2017): 430–56.
- Bailey, Michael A., and Erik Voeten. “A Two-Dimensional Analysis of Seventy Years of United Nations Voting.” *Public Choice* 176 (2018): 3355.
- Barnes, Julian E. “U.S. Cyberattack Hurt Iran’s Ability to Target Oil Tankers, Officials Say.” *The New York Times*, August 28, 2019, sec. U.S.
- Barrie, Douglas. “Trends in Missile Technologies.” *I/SS* (blog), March 2019.

- Baumeister, R. F., E. Bratslavsky, C. Finkenauer, and K. D. Vohs. "Bad Is Stronger than Good." *Review of General Psychology* 5 (2001): 323–70.
- Beatrix Immenkamp, Gianluca Sgueo, Sofija Voronova, and Alina Dobрева. "The Fight against Terrorism." European Parliament, June 2019.
- Bechev, Dimitar. *Understanding Russia's Influence in the Western Balkans*. The European Center of Excellence for Countering Hybrid Threats, 2018.
- Beirut, Dan Roberts Kareem Shaheen in, and agencies. "Saudi Arabia Launches Yemen Air Strikes as Alliance Builds against Houthi Rebels." *The Guardian*, March 26, 2015, sec. World news.
- Bekkers, Frank, Rick Meessen, and Deborah Lassche. "Hybrid Conflicts: The New Normal?" The Hague, Netherlands: TNO, December 2018.
- Ben Wagner, Joanna Bronowicka, Cathleen Berger, and Thomas Behrndt. "Surveillance and Censorship: The Impact of Technologies on Human Rights." European Parliament. Accessed December 6, 2019.
- Bentzen, Naja. "Foreign Influence Operations in the EU." Members' Research Service, July 2018.
- Berman, Ilan. "Technology Is Making Terrorists More Effective—And Harder to Thwart." *The National Interest*, February 22, 2019.
- Binnendijk, Hans. "Friends, Foes, and Future Directions: U.S. Partnerships in a Turbulent World: Strategic Rethink." Product Page, 2016.
- Blume, Susanna V., and Lauren Fish. "Overview of the 2019 President's Budget Request for Defense." Center for a New American Security (CNAS), February 15, 2018.
- Bob Johansen. *Get There Early: Sensing the Future to Compete in the Present*, 2007.
- Bordoff, Jason, and Trevor Houser. *American Gas to the Rescue? The Impact of US LNG Exports on European Security and Russian Foreign Policy*. New York, United States of America: Columbia University, 2014.
- Borger, Julian. "Trump Issues New Sanctions on North Korea and Claims China Is Following." *The Guardian*. September 21, 2017.
- Bornschieer, Simon, and Hanspeter Kriesi. "The Populist Right, the Working Class, and the Changing Face of Class Politics," 10–29, 2013.

- Bowcott, Owen. "Beijing Rejects Tribunal's Ruling in South China Sea Case." *The Guardian*, July 12, 2016, sec. World news.
- Boy, John D., and Justus Uitermark. "Reassembling the City through Instagram." *Transactions of the Institute of British Geographers* 42, no. 4 (2017): 612–624.
- Bradshaw, Samantha, and Philip Howard. "The Global Disinformation Order: 2019 Global Inventory Of Organised Social Media Manipulation." Working Paper. Oxford, United Kingdom: Oxford Internet Institute, 2019.
- Brands, Hal. "Paradoxes of the Gray Zone - Foreign Policy Research Institute." *FPRI* (blog), February 5, 2016.
- Branko Milanovic. "Description of All the GINIS Dataset." Stone Center on Socio-Economic Inequality, 2019.
- Braumoeller, Bear F. *Only the Dead: The Persistence of War in the Modern Age*. Oxford University Press, 2019.
- Brenna Smith. "The Evolution Of Bitcoin In Terrorist Financing." *Bellingcat* (blog), August 9, 2019.
- Broad, William J., and David E. Sanger. "Race for Latest Class of Nuclear Arms Threatens to Revive Cold War." *The New York Times*, April 16, 2016, sec. Science.
- Brockmann, K, Bauer, S, and Boulanin, V. "Arms Control and the Convergence of Biology and Emerging Technologies." SIPRI, March 2019.
- Bruce Schneier. "The Psychology of Security." Springer-Verlag Berlin Heidelberg, 2008.
- Bulletin of the Atomic Scientists. "Doomsday Clock - Timeline." *Bulletin of the Atomic Scientists* (blog), 2019.
- Byman, Daniel L. "Why Engage in Proxy War? A State's Perspective." *Brookings* (blog), May 21, 2018.
- Byun, See-Won. "China's Major-Powers Discourse in the Xi Jinping Era: Tragedy of Great Power Politics Revisited?" *Asian Perspective* 40, no. 3 (2016): 493–522.
- "Call to Protect the Electoral Infrastructure." The Global Commission on the Stability of Cyberspace (GCSC), 2018.

“Call to Protect the Public Core of the Internet.” The Global Commission on the Stability of Cyberspace (GCSC), 2017.

Cameron, David. “David Cameron’s Full Statement Calling for UK Involvement in Syria Air Strikes,” November 26, 2015, sec. News.

Campos, Rodrigo. “Human Rights Chief Slams Security Council for Inaction on Syria.” *Reuters*, March 20, 2018.

“Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua vs. United States of America),” June 1986.

Cat Cronin. “Weaponizing Technology: 21st Century Terrorism.” American Security Project, June 2019.

Catherine De Bolle, Executive. “Internet Organised Crime Threat Assessment 2018.” Europol, 2018.

Center for Systemic Peace. “Polity IV Project, Political Regime Characteristics and Transitions, 1800–2018.” Integrated Network for Societal Conflict Research (INSCR), July 27, 2019.

Chan, Minni. “What’s Driving China’s Military Modernisation Push?” *South China Morning Post*, August 1, 2017.

“Charter of the United Nations,” August 10, 2015.

Chesney, Robert, and Danielle Citron. “Disinformation on Steroids: The Threat of Deep Fakes.” *Cyber Brief*. Council for Foreign Relations, October 16, 2018.

“China’s National Defense in the New Era.” “China’s National Defense in the New Era” (The State Council Information Office of the People’s Republic of China, 2019).

“Chinese Public Diplomacy in Taiwan.” NATO Strategic Communications Center of Excellence, June 2019.

Christiaan Pelgrim, and Clara van de Wiel. “Handelsconflict VS En EU Bedreigt Wereldeconomie.” *NRC*, October 2019.

Christopher Bronk, and Eneken Tikk-Ringas. “The Cyber Attack on Saudi Aramco.” *Survival* 55, no. 2 (April 2013): 81–96.

Claire Graja. "SOF and the Future of Global Competition." CNA, May 2019.

Clapper, James R., Marcel Lettre, and Michael S. Rogers. "Joint Statement for the Record to the Senate Armed Services Committee Foreign Cyber Threats to the United States." U.S. Senate Armed Services Committee, January 5, 2017.

Coats, Daniel R. "Statement for the Record." Worldwide Threat Assessment of the US Intelligence Community. Washington, D.C.: Senate Select Committee on Intelligence, 2019.

"Coding Rubric and Anchor Texts for the Global Populism Database." The Guardian, March 5, 2019.

Collier, Paul, Elliott, V. L., Hegre, Håvard, Hoeffler, Anke, Reynal-Querol, Marta, and Sambanis, Nicholas. "Breaking the Conflict Trap : Civil War and Development Policy." World Bank, 2003.

"Communication from the Commission on a European Union Programme for Critical Infrastructure Protection." European Union Commission, December 12, 2006.

Connolly, Richard, and Mathieu Boulègue. "Russia's New State Armament Programme." Chatham House, May 2018.

Cooper, Julian. "Russia's State Armament Programme to 2020: A Quantitative Assessment of Implementation 2011-2015," 2016.

Coppedge, Michael, John Gerring, Carl Henrik Knutsen, Staffan I. Lindberg, Jan Teorell, David Altman, Michael Bernhard, et al. "V-Dem Codebook V9." Varieties of Democracy (V-Dem) Project, 2019.

Cordesman, Anthony. *Chinese Strategy and Military Modernization in 2016: A Comparative Analysis*. Washington D.C., USA: Center for Strategic & International Studies, 2016.

Corre, Philippe Le. "China's Golden Era in Portugal." Carnegie Endowment for International Peace, November 24, 2018.

Transparency International. "Corruption Perceptions Index 2018." Accessed December 11, 2019.

"Corruption Perceptions Index 2018: Technical Methodology Note." Transparency International, 2018.

- Time. “Could China Develop Killer Robots in the Near Future? Experts Fear So.” Accessed October 31, 2019.
- “Country Views on Killer Robots.” Campaign To Stop Killer Robots, November 22, 2018.
- Cyber Attacks Controlled by Intelligence Services*. Bundesamt für Verfassungsschutz, 2018.
- Council on Foreign Relations. “Cyber Operations Tracker.” Accessed December 20, 2019.
- Daalder, Ivo H., and James M. Lindsay. *The Empty Throne: America’s Abdication of Global Leadership*. New York: Public Affairs, 2018.
- Dahir, Abdi Latif. “Russia Is the Latest World Power Eyeing the Horn of Africa.” Quartz Africa, March 9, 2018.
- Dan Smith. “The US Withdrawal from the Iran Deal: One Year on | SIPRI.” *SIPRI* (blog), May 2019.
- Daniel Coats. “Worldwide Threat Assessment of the US Intelligence Community.” Senate Select Committee on Intelligence, January 29, 2019.
- Danny Pronk. “The Return of Political Warfare | Strategic Monitor 2018–2019.” Clingendael, 2018.
- Daryl G. Kimball. “Bolton’s Attempt to Sabotage New START | Arms Control Association.” Arms Control Association, August 2019.
- Daryl Kimball. “The Trump Administration’s Failing Iran Policy Is Spurring Troubling Retaliatory Actions by Iran.” Arms Control Association. Accessed December 20, 2019.
- Daveed Gartenstein. “Terrorists Are Going to Use Artificial Intelligence.” *Defense One*, May 2018.
- Davenport, Kelsey. “Chronology of U.S.–North Korean Nuclear and Missile Diplomacy | Arms Control Association.” Arms Control Association – Fact Sheets & Briefs, October 2019.
- David Ibsen. “Big Tech Spends Millions to Shape Possible Regulation of Extremist Content Online.” *Counter Extremism Project* (blog), May 8, 2019.

- Daws, Ryan. "Putin Outlines Russia's National AI Strategy Priorities." *AI News* (blog), May 31, 2019.
- Dawson, Linda. *War in Space: The Science and Technology Behind Our Next Theater of Conflict*. Springer, 2019.
- "De Nederlandse Importafhankelijkheid van China, Rusland En de VS." Centraal Bureau voor de Statistiek, November 2019.
- De Spiegeleire, Stephan, Kars De Bruijne, Frank Bekkers, Minke Meijnders, and Tim Sweijs. "Stilte Voor de Storm?," 2018.
- De Spiegeleire, Stephan, Khrystyna Holynska, and Yevhen Sapolovych. "Things May Not Be as They Seem: Geo-Dynamic Trends in the International System," 2018.
- "Definition of the Public Core." The Global Commission on the Stability of Cyberspace (GCSC), 2018.
- Dennis Blair. "Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence." Director of National Intelligence, February 2009.
- Dion-Schwarz, Cynthia, David Manheim, and Patrick B. Johnston. "Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats." Product Page. RAND Corporation, 2019.
- Dockrill, Peter. "Chilling New Research Shows How Dire a Smallpox Bioterror Attack Could Actually Get." *ScienceAlert*, February 2019.
- Doffman, Zak. "Warning Over Terrorist Attacks Using Drones Given By EU Security Chief." *Forbes*, August 2019.
- Dollar, David. "The AIIB and the 'One Belt, One Road.'" *Brookings* (blog), June 21, 2015.
- Donald Gasper. "China and Russia Want to Develop Arctic Energy Resources Together, and US Disapproval May Not Deter Them | South China Morning Post." *South China Morning Post*, September 2018.
- Doran, Charles F. "Economics, Philosophy of History, and the 'Single Dynamic' of Power Cycle Theory: Expectations, Competition, and Statecraft." *International Political Science Review* 24, no. 1 (January 1, 2003): 13–49.
- Douglas Barrie. "Ground-Launched Cruise Missiles, Europe and the End of the INF Treaty?" *IISS* (blog), February 2019.

- Downman, M, and Messmer, M. “Re-Emerging Nuclear Risks in Europe: Mistrust, Ambiguity, Escalation and Arms-Racing between NATO and Russia.” The British American Security Information Council, April 2019.
- Dustin Volz. “U.S. Blames North Korea for ‘WannaCry’ Cyber Attack.” *Reuters*, December 2017.
- “Economists Are Rethinking the Numbers on Inequality.” *The Economist*, November 28, 2019.
- E.E. Duchateau-Polkerman. “EMSD Thesis De Perceptie van Veiligheid.” Hogere Defensie Vorming, 2015.
- Middle East Monitor. “Egypt’s Sisi Approves Establishment of Russia Industrial Zone,” February 1, 2019.
- Einsiedel, Sebastian von. “Civil War Trends and the Changing Nature of Armed Conflict.” *United Nations University*, 2017.
- The Economist Intelligence Unit. “EIU Global Forecast - Geopolitics Threatens Global ICT Order,” February 13, 2019.
- Elias Groll. “Did Russia Knock Out Ukraine’s Power Grid? – Foreign Policy.” *Foreign Policy*, January 2016.
- Ellen Nakashima, and David Lynch. “U. S. Charges Chinese Hackers in Alleged Theft of Vast Trove of Confidential Data in 12 Countries.” *MSN*, December 21, 2018.
- Ellick, Adam B., and Adam Westbrook. “Opinion | Operation Infektion: A Three-Part Video Series on Russian Disinformation.” *The New York Times*, November 12, 2018.
- Elsa Kania. “China May Soon Surpass America on the Artificial Intelligence Battlefield.” *The National Interest* (blog), February 21, 2017.
- “Emmanuel Macron in His Own Words (English).” *The Economist*. November 26, 2016.
- Organization for Security and Co-operation in Europe (OSCE). “Ensuring Military Transparency – the Vienna Document.” Accessed September 19, 2019.
- Errol van Engelen. “Big Data Will Effectively Fight Terrorism In The World.” *Datafloq*, January 2019.
- European Commission. “EU Budget for the Future.” Text, 2018.

“EU Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection.” Official Journal of the European Union, December 8, 2008.

Trade - European Commission. “EU Foreign Investment Screening Regulation Enters into Force,” April 2019.

European Commission. “EU Sanctions Map: Russia,” July 2019.

European Commission - European Commission. “EU-China Strategic Outlook: Commission and HR/VP Contribution to the European Council.” Text, March 21, 2019.

Eva Entenmann. “Terrorist Financing and Virtual Currencies: Different Sides of the Same Bitcoin?” *ICCT*, November 1, 2018.

Fariss, Christopher. “Yes, Human Rights Practices Are Improving Over Time,” May 27, 2019.

Fei Su, and Ian Anthony. “Reassessing CBRN Threats in a Changing Global Environment.” *SIPRI* (blog), June 2019.

Fernholz, Tim. “Jeff Bezos Says Space Isn’t a Race. We’re Not so Sure.” Quartz. Accessed December 9, 2019.

“For Decades, the United States and Russia Stepped Back From the Brink. Until Now.” *The New York Times*, February 10, 2019, sec. Opinion.

Foreign & Commonwealth Office, and National Cyber Security Centre. “Press Release: UK Exposes Russian Cyber Attacks.” GOV.UK, October 4, 2018.

NATO. “Foreign Ministers Take Decisions to Adapt NATO, Recognize Space as an Operational Domain, 20-Nov.-2019,” November 2019.

“Forming Coalitions in the EU after Brexit: Alliances for a European Union That Modernises and Protects.” Publicatie. Advisory Council on International Affairs, July 6, 2018.

“Framework for Improving Critical Infrastructure Cybersecurity.” National Institute of Standards and Technology, April 16, 2018.

- Franck, Thomas M. "Who Killed Article 2(4)? Or: Changing Norms Governing the Use of Force by States." *The American Journal of International Law* 64, no. 5 (1970): 809–37.
- Freedom House. "Freedom in the World 2019: Democracy in Retreat." Freedom in the World 2019, January 15, 2019.
- Funke, Daniel, and Daniela Flamini. "A Guide to Anti-Misinformation Actions around the World." Poynter, 2018.
- Gallup International Association. "Voice of the People 2015." Accessed December 9, 2019.
- Gallup Pakistan. "WIN/Gallup International's Global Survey Shows Three in Five Willing to Fight for Their Country." Press Release, March 18, 2015.
- Garamone, Jim, and Lisa Ferdinando. "DoD Initiates Process to Elevate U.S. Cyber Command to Unified Combatant Command." *U.S. Department of Defense*, August 18, 2017.
- Gearan, Ann. "Trump's Dual Instincts on Iran: Big Threats and an Eagerness to Deal." Washington Post, 2019.
- Geoffrey Ingersoll. "China Hacking: P.L.A. Unit 61398." *Business Insider*. Accessed November 7, 2019.
- Gibas-Krzak, Danuta. "The Political, Economic and Cultural Influences of Neo-Ottomanism in Post-Yugoslavian Countries. An Analysis Illustrated with Selected Examples." *POLSKA AKADEMIA UMIEJĘTNOŚCI* 26 (2017).
- Gils, van, S. "Deltawerken En Sluizen Kwetsbaar Voor Cyberaanvallen." FD.nl, March 2019.
- "GINI Index (World Bank Estimate) - South Africa | Data." Accessed November 26, 2019.
- Global Commission on the Stability of Cyberspace. "Norm against Offensive Cyber Operations by Non-State Actors." In *Norm Package Singapore*, 2018.
- Inequality.org. "Global Inequality." Accessed November 21, 2019.
- "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace." Organization for Security and Co-operation in Europe (OSCE), 2013.

- Gordon Corera. "Looking for China's Spies." *BBC News*, December 2018.
- Goswami, Namrata. "The Moon's Far Side and China's Space Strategy." Accessed December 9, 2019.
- Graves, Tom. Active Cyber Defense Certainty Act, Pub. L. No. H.R. 3270 (2019).
- Haas Institute for a Fair and Inclusive Society. "2018 Inclusiveness Index," December 2018.
- Hegel, Chuck. Reagan National Defense Forum Keynote (2014).
- Henry Kissinger. *World Order*, 2014.
- Heywood, Andrew. *Political Theory: An Introduction*. Macmillan International Higher Education, 2015.
- Holden, Emily. "Trump Begins Year-Long Process to Formally Exit Paris Climate Agreement." *The Guardian*, November 5, 2019, sec. US news.
- Hongchan Chun. "Russia's Energy Diplomacy toward Europe and Northeast Asia: A Comparative Study." *Asia Europe Journal*, 2009.
- Hopkin, Jonathan, and Mark Blyth. "The Global Economics of European Populism: Growth Regimes and Party System Change in Europe." *Government and Opposition* 54, no. 2 (April 2015): 193–225.
- Hornby, Lucy, Michael Peel, Davide Ghiglione, and Demetri Sevastopulo. "Italy Set to Formally Endorse China's Belt and Road Initiative." *Financial Times*, March 6, 2019.
- Hosli, Madeleine O., Evelyn van Kampen, Frits Meijerink, and Katherine Tennis. "Voting Cohesion in the United Nations General Assembly: The Case of the European Union." Porto, Portugal, 2010.
- Høvring, Roald. "10 Things to Know about the Crisis in Yemen." NRC. Accessed November 25, 2019.
- World Economic Forum. "How Emerging Technologies Increase the Threat from Biological Weapons," March 2019.
- "Huawei Mag Meebouwen Aan 5G-Netwerken in Duitsland." *NOS*, October 14, 2019.

Hugo van Manen, Koen van Wijk, Elisabeth Dick, and Tim Sweijs. “Methodological Note - The Dutch Foreign Relations Index: Version 2.” Hague Centre for Strategic Studies, January 2020.

Hugo van Manen, Koen van Wijk, Juliette Schaffrath, and Tim Sweijs. “Methodological Annex: What World Do We Live In?” Hague Centre for Strategic Studies, January 2020.

“Human Development Reports - 2018 Statistical Update,” 2018.

Human Rights Watch. “ILO: New Treaty to Protect Workers from Violence, Harassment.” Human Rights Watch, June 21, 2019.

Hybrid Threats: A Strategic Communications Perspective. Riga, Latvia: NATO Centre of Excellence, 2019.

Ikenberry, John. “The End of Liberal International Order?” *International Affairs* 94, no. 1 (January 1, 2018): 7–23.

International Chamber of Commerce. “IMB Piracy Report 2018: Attacks Multiply in the Gulf of Guinea,” January 2019.

“Independent International Fact-Finding Mission on the Conflict in Georgia,” 2009.

Inglehart, Ronald F, Bi Puranen, and Christian Welzel. “Declining Willingness to Fight for One’s Country: The Individual-Level Basis of the Long Peace.” *Journal of Peace Research* 52, no. 4 (March 7, 2015): 418–34.

“Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, Decision No. 1106.” Organization for Security and Co-operation in Europe (OSCE), 2013.

Institute for Economics and Peace. “Global Peace Index 2019,” 2019.

Global Defence Technology. “Intelligent Design: Inside France’s € 1.5bn AI Strategy - Global Defence Technology | Yearbook 2018,” 2019.

Interpol. “INTERPOL and UN Publish Joint Handbook for Online Counter-Terrorism Investigations,” July 2019.

Iryna Bogdanova. “WTO Dispute on the US Human Rights Sanctions Is Looming on the Horizon.” *EJIL: Talk!* (blog), January 2019.

- Istrate, Dominik. “Nord Stream 2 must be stopped, EU parliament says.” *Emerging Europe*, March 14, 2019.
- Jakob Hanke, and Jacopo Barigazzi. “EU Accelerates Moves to Block China’s Market Access.” *POLITICO*, March 18, 2019.
- James Acton. “The Weapons Making Nuclear War More Likely.” *BBC News*, February 2019.
- Jeangene Vilmer, Jean-Baptiste, Alexandre Escorcica, Marine Guillaume, and Janaina Herrera. “Information Manipulation: A Challenge for Our Democracies.” Paris, France: Policy Planning Staff of the Ministry for Europe & Foreign Affairs and the Institute for Strategic Research at the Ministry for the Armed Forces, August 2018.
- Jinping, Xi. “Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era.” *Qiushi Journal*. Accessed December 9, 2019.
- Jo Harper. “Kaliningrad Gets Moscow Energy Boost as Baltic States Pull Plug.” *DW.COM*, March 22, 2019.
- Johannes Thimm. “From Exception to Normalcy.” *SWP - Stiftung Wissenschaft und Politik/German Institute for International and Security Affairs*, October 2018.
- John Borrie, Amy Dowler, and Pavel Podvig. “Hypersonic Weapons: A Challenge and Opportunity for Strategic Arms Control.” *UNODA* (blog), February 2019.
- Johnson, Larry. “Automated Cyber Attacks Are the Next Big Threat. Ever Hear of ‘Review Bombing’?” *Entrepreneur*, December 21, 2018.
- Johnson, Tierney. “Bad World: The Negativity Bias in International Politics.” *International Security* 43, no. 3 (2019).
- Jonathan E. Hillman. “Corruption Flows Along China’s Belt and Road.” *CSIS* (blog), January 18, 2019.
- Jones, Bruce, and Torrey Taussig. “Democracy & Disorder: The Struggle for Influence in the New Geopolitics.” *Brookings*, February 2018.
- Joshua A. Geltzer, Karen Kornbluh, and Nicholas Rasmussen. “Tech Companies Must Fight White Supremacy, Regardless of Political Dangers.” *Lawfare*, August 7, 2019.

- Julian Cooper. “The Funding of Nuclear Weapons in the Russian Federation.” Centre Pembroke College, University of Oxford n, October 2018.
- Julian L. Simon. *The State of Humanity*, 1996.
- Jushkin, Vladimir. “What Is Hidden in Russia’s Military Budget.” ICDS. Accessed December 9, 2019.
- Kahneman, Daniel. *Thinking, Fast and Slow*. 1st edition. New York: Farrar, Straus and Giroux, 2013.
- Kars De Bruijne. “Vitale Belangen.” Clingendael, 2018.
- Katani, Tetsuo. “China and Russia in the Western Pacific: Implications for Japan and the United States.” *The National Bureau of Asian Research (NBR)* (blog). Accessed December 9, 2019.
- Kathleen McKendrick. “Artificial Intelligence Prediction and Counterterrorism.” Chatham House, August 2019.
- Ke, Xu, Priyanka Saksena, and Alberto Holly. “The Determinants of Health Expenditure: A Country-Level Panel Data Analysis.” *World Health Organisation*, 2011, 28.
- Keegan Elmer. “Europe’s China Problem Is on the Agenda at next European Commission Meeting.” *South China Morning Post*, February 27, 2019.
- Keith Schnakenberg, and Christopher Fariss. “Dynamic Patterns of Human Rights Practices.” *Political Science Research and Methods*, April 2014.
- Kim, Dong-Hun. “Coercive Assets? Foreign Direct Investment and the Use of Economic Sanctions.” *International Interactions* 39, no. 1 (January 1, 2013): 99–117.
- Kimball, Daryl. “The Open Skies Treaty at a Glance.” Arms Control Association, October 2012.
- Klimburg, Alexander, and Louk Faesen. “A Balance of Power in Cyberspace | HCSS.” *European Cybersecurity Journal* 3, no. 4 (2018).
- Koh, Harold H. “International Law in Cyberspace.” presented at the USCYBERCOM Inter-Agency Legal Conference, Fort Meade, Maryland, September 18, 2012.
- Kovrig, Michael. “China Expands Its Peace and Security Footprint in Africa.” *Crisis Group* (blog), October 24, 2018.

- Langman, Jimmy. "From Model to Muddle: Chile's Sad Slide Into Upheaval." *Foreign Policy* (blog), 2019.
- Lauren Williams. "Cyber Command Looks to Expand." FCW, February 2019.
- Laurence Bindner, and Raphael Gluck. "Trends in Islamic State's Online Propaganda: Shorter Longevity, Wider Dissemination of Content." *ICCT*, December 5, 2018.
- Lebow, Richard Ned, and Benjamin Valentino. "Lost in Transition: A Critical Analysis of Power Transition Theory." *International Relations* 23, no. 3 (September 1, 2009): 389–410.
- Leone, Dario. "Did Russia's Deadly Su-57 Stealth Fighter Get Ready for 'War' in Syria?" *The National Interest*, August 31, 2019.
- Lisbeth Kirk. "Europe Shifts Gear to Balance Relations with China Better." *EUobserver*, March 13, 2019.
- "List of All Cases | International Court of Justice." Accessed October 23, 2019.
- Louk Faesen, Bianca Torossian, Elliot Mayhew, and Carlo Zensus. "Conflict in Cyberspace: Parsing the Threats and the State of International Order in Cyberspace." HCSS, November 2019.
- Lukas Trakimavičius. "The Threat of AI to Energy Security." RealClearDefense, December 7, 2018.
- Ma, Alexandra. "This Is China's Playbook to Pit EU Countries against Each Other." *Business Insider*, March 24, 2019.
- Mads Frese. "Italy Takes China's New Silk Road to the Heart of Europe." *EUobserver* (blog), March 2019.
- Mair, Peter. *Ruling the Void: The Hollowing out of Western Democracy*. New York City: Verso, 2013.
- Maizland, Lindsay. "China's Repression of Uighurs in Xinjiang." Council on Foreign Relations, November 25, 2019.
- Malte Humpert. "China Launches Domestically-Built 'Xue Long 2' Icebreaker." *High North News*, September 11, 2018.

- Maria Kiselyova. "Russia Warns of Repeat of 1962 Cuban Missile Crisis." *Reuters*, June 24, 2019.
- Marshall, Abbey. "Erdogan Says He Returned Trump's Threatening Letter on Syria Invasion." *POLITICO*, 2019.
- Martyn Frampton, Ali Fisher, and Nico Prucha. "The New Netwar: Countering Extremism Online." *Policy Exchange* (blog), September 23, 2017.
- Mattis, Peter. "China's 'Three Warfares' in Perspective." *War on the Rocks* (blog), January 30, 2018.
- Maxamuud Axmed. "Egypt, Somalia Bolster Security Coordination Amid Suez Canal Fears. | Somaliweyn." *Somaliweyn*, March 2019.
- Mazarr, Michael J., Jonathan S. Blake, Abigail Casey, Tim McDonald, Stephanie Pezard, and Michael Spirtas. *Understanding the Emerging Era of International Competition: Theoretical and Historical Perspectives*. RAND Corporation, 2018.
- McGrath, Matt. "Putin: Russian President Says Liberalism 'Obsolete.'" *BBC News*, June 28, 2019, sec. Europe.
- Mearsheimer, John J. "Bound to Fail: The Rise and Fall of the Liberal International Order." *International Security* 43, no. 4 (April 1, 2019): 7–50.
- Freedom House. "Methodology 2019," January 15, 2019.
- Human Rights Watch. "#MeToo Movement's Second Anniversary," October 14, 2019.
- Michael Nienaber. "U.S. Warns German Companies of Possible Sanctions over Russian Pipeline." *Reuters*, January 13, 2019.
- Michael Shurkin. "The Abilities of the British, French, and German Armies to Generate and Sustain Armored Brigades in the Baltics." Research Report. RAND Corporation, 2017.
- Michael T. Klare. "An 'Arms Race in Speed': Hypersonic Weapons and the Changing Calculus of Battle," June 2019.
- Milanovic, Branko. "Description of All the GINIS Dataset." Stone Center on Socio-Economic Inequality, 2019.

“Military and Security Developments Involving the People’s Republic of China 2019.”
US. Dept. of Defense, May 2, 2019.

Ministry for Europe and Foreign Affairs of France. “Paris Call for Trust and Security in
Cyberspace,” November 12, 2018.

Ministry of Foreign Affairs. “Working Worldwide for the Security of the Netherlands:
An Integrated International Security Strategy 2018-2022.” Ministry of Foreign
Affairs, March 20, 2018.

SIPRI. “Modernization of World Nuclear Forces Continues despite Overall Decrease in
Number of Warheads,” June 17, 2019.

Mohammed Haddad, Usaid Siddiqui, and Owais Zaheer. “How Has My Country Voted at
the UN?” Al Jazeera. Accessed December 9, 2019.

Morris, Lyle J., Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika
Binnendijk, and Marta Kepe. “Gaining Competitive Advantage in the Gray Zone:
Response Options for Coercive Aggression Below the Threshold of Major War.”
Product Page. RAND Corporation, 2019.

Mounk, Yascha. “Bolivia Should Worry Autocrats Everywhere.” The Atlantic, 2019.

Moyer, Jonathan D., Tim Sweijs, Mathew J. Burrows, and Hugo van Manen. “Power and
Influence in a Globalized World.” Washington, DC: Atlantic Council, Frederick S.
Pardee Center for International Futures and HCSS, January 2018.

Mozur, Paul. “One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a
Minority.” *The New York Times*, April 14, 2019, sec. Technology.

Mueller, Robert. “Report On The Investigation Into Russian Interference In The 2016
Presidential Election.” Washington D.C., USA: U.S. Department of Justice, March
2019.

Internet Society. “Mutually Agreed Norms for Routing Security (MANRS) for Network
Operators (ISP) and for Internet Exchange Points (IXP).” Accessed September 4,
2019.

Nate Schenkkan, and Sarah Repucci. “The Freedom House Survey for 2018: Democracy
in Retreat.” *Journal of Democracy*, April 2019.

“National Security Strategy and Strategic Defence and Security Review 2015: A Secure
and Prosperous United Kingdom.” Her Majesty’s Government, November 2015.

- “National Security Strategy and Strategic Defence and Security Review 2015: First Annual Report 2016.” Her Majesty’s Government, December 2016.
- “NATO: Suspension of Treaty Is Step in Wrong Direction – World News – Jerusalem Post.” Accessed October 23, 2019.
- Névine Schepers. “Q&A: Understanding Saudi Arabia’s Nuclear Energy Programme.” *IJSS* (blog), April 30, 2019.
- Ni, Adam, and Bates Gill. “The People’s Liberation Army Strategic Support Force: Update 2019.” *China Brief*, May 29, 2019.
- Ni Aolian. “European Counter-Terrorism Approaches: A Slow and Insidious Erosion of Fundamental Rights.” *Just Security*, October 17, 2018.
- Nicholas Schmitt. “Rule 10—Prohibition of Threat or Use of Force.” In *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2013.
- Nicholas Tsagourias. “Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace.” *EJIL: Talk!* (blog). Accessed December 11, 2019.
- “Nuclear Posture Review 2018.” U.S. Department of Defense, 2018.
- O’Connor, Nat. “Three Connections between Rising Economic Inequality and the Rise of Populism.” *Irish Studies in International Affairs* 28 (2017): 29–43.
- Ortiz-Ospina, Esteban, and Max Roser. “Government Spending.” *Our World in Data*, 2016.
- Panda, Ankit. “From Hardware to Software: China’s 2019 Military Budget and Priorities.” *The Diplomat*, March 17, 2019.
- Paris, Britt, and Joan Donovan. “Deepfakes and Cheap Fakes.” *United States of America: Data & Society*, October 18, 2019.
- “Paris Call for Trust and Security in Cyberspace – Paris Call.” Accessed December 9, 2019.
- Patrick M. Regan, and Sam R. Bell. “Changing Lanes or Stuck in the Middle: Why Are Anocracies More Prone to Civil Wars?,” 2010.
- Patrick Tucker. “Big Tech Bulks Up Its Anti-Extremism Group. But Will It Do More than Talk?” *Defense One*, September 2019.

- Patrick, Wintour. "Nato to Consider Expert Panel after Macron Brain-Dead Claim." *The Guardian*. November 26, 2019.
- Peter Diamandis. "Abundance: The Future Is Better Than You Think," 2013.
- Pew Research Center. "How Religious Restrictions Have Risen Around the World." *Pew Research Center's Religion & Public Life Project* (blog), July 15, 2019.
- Pierson, Paul. *Politics in Time: History, Institutions, and Social Analysis*. Princeton University Press, 2011.
- Pinker, Steven. *Enlightenment Now: The Case for Reason, Science, Humanism, and Progress*. 1st Edition. New York, New York: Viking, 2018.
- Pinnell, Owen. "The Online War between Qatar and Saudi Arabia." BBC News, June 3, 2018.
- Pollpeter, Kevin, Michael Chase, and Eric Heginbotham. "The Creation of the PLA Strategic Support Force and Its Implications for Chinese Military Space Operations." Research Reports. California, United States of America: RAND Corporation, 2017.
- Polyakova, Alina, and Daniel Fried. "Democratic Defense Against Disinformation 2.0." Washington D.C., USA: Atlantic Council, June 2019.
- President of the United States of America. "National Security Strategy of the United States of America." The White House, 2017.
- The White House. "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.
- Press, Associated. "Ecuador Protests End after Deal Struck with Indigenous Leaders." *The Guardian*, October 14, 2019, sec. World news.
- "Protecting Critical Energy Infrastructure from Terrorist Attack, Decision No. 6/07." Organization for Security and Co-operation in Europe (OSCE), 2007.
- "Putin to Trump: We'll Develop New Nuclear Missiles If You Do." *Reuters*, August 5, 2019.
- Putin, Vladimir. "The Military Doctrine of the Russian Federation." Military Doctrine, December 25, 2014.

- Putnam, Robert. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster, 2000.
- Ranger, Steve. “Cyberattacks: China and Russia Can Disrupt US Power Networks Warns Intelligence Report.” *ZDNet*, January 2019.
- Rebecca Arcesati. “Chinese Tech Standards Put the Screws on European Companies.” Mercator Institute for China Studies, January 2019.
- Renz, Bettina. “Russia and ‘Hybrid Warfare.’” *Contemporary Politics* 22, no. 3 (July 2, 2016): 283–300.
- “Repertoire of the Practice of the Security Council.” United Nations, 2015 2014.
- “Repertoire of the Practice of the Security Council.” United Nations, 2017 2016.
- Republic of France. “Defence and National Security: Strategic Review 2017,” 2017.
- “Resolution 2249 (2015) Adopted by the Security Council at Its 7565th Meeting, on 20 November 2015.” United Nations Security Council, November 20, 2015.
- Responsibility of States for Internationally Wrongful Acts (2001).
- Reynold, Anna. *Redefining Euro-Atlantic Values: Russia’s Manipulative Techniques*. Riga, Latvia: NATO Strategic Communications Center of Excellence, 2017.
- Richard Spencer. “Stuxnet Virus Attack on Iranian Nuclear Programme: The First Strike by Computer? - Telegraph.” *The Telegraph*, October 2010.
- Richard Wike, and Janell Fetterolf. “Liberal Democracy’s Crisis of Confidence.” *Journal of Democracy*, October 2018.
- Al Jazeera. “Rights Group: Deadly Attacks on Sudan Protesters Were Planned,” 2019.
- Rijksoverheid. “NCTV: Dreigingsniveau Naar 3, Aanslag in Nederland Voorstelbaar,” December 2019.
- Riqiang, Wu. “Trilateral Arms Control Initiative: A Chinese Perspective.” *Bulletin of the Atomic Scientists* (blog), September 4, 2019.
- Rita Katz. “A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps.” *Wired*, January 9, 2019.

Roache, Madeline. "Central And Eastern Europeans Believe Democracy Is Under Threat, Poll Finds." *Time*, April 11, 2019.

Robert Einhorn, and Richard Nephew. "Constraining Iran's Future Nuclear Capabilities." *Brookings* (blog), March 26, 2019.

Roser, Max, Hannah Ritchie, and Esteban Ortiz-Ospina. "Internet." *Our World in Data*, 2019.

"Routing Security for Policymakers - An Internet Society White Paper." The Internet Society, October 2018.

Rrustemi, Arlinda, et al. "Geopolitical Influences of External Powers in the Western Balkans." HCSS Security, September 30, 2019.

"Russia Announces Establishing Industrial Zone in Egypt in 2021." *EgyptToday*, February 2019.

"Russia Expels 755 US Diplomats in Response to Sanctions." *Al Jazeera*, July 30, 2017.

ETHZ. "Russia: National Security Strategy to 2020," May 2009.

Russia, Team of the Official Website of the President of. "Address by President of the Russian Federation." President of Russia. Accessed October 22, 2019.

"Russian National Security Strategy," December 2015.

"Russia's Withdrawal from CFE Treaty Work a 'dangerous Move,' Says OSCE PA Security Chair | OSCE." Accessed October 16, 2019.

Safi, Michael. "Frustration and Anger Fuel Wave of Youth Unrest in Arab World." *The Observer*, November 2, 2019, sec. World news.

Sanger, David E., and Steven Lee Myers. "After a Hiatus, China Accelerates Cyberspying Efforts to Obtain U.S. Technology." *The New York Times*, November 29, 2018, sec. U.S.

Sarah March. "US Joins UK in Blaming Russia for NotPetya Cyber-Attack." *The Guardian*, February 2015.

Schmitt, Michael N., and Liis Vihul. "Proxy Wars in Cyber Space: The Evolving International Law of Attribution." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, May 31, 2014.

- Schrodt, Philip. "CAMEO Conflict and Mediation Event Observations Event and Actor Codebook." Pennsylvania State University, 2012.
- Scott Stewart. "A Sting Operation Lifts the Lid on Chinese Espionage." *Stratfor* (blog), October 2018.
- Sensenbrenner, James F. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT), Pub. L. No. H.R.3162 (2001).
- Serrano, Francisco. "After 8 Months on the Streets, Protesters in Algeria Aren't Giving Up." *Foreign Policy* (blog), 2019.
- Seth Harrison. "Evolving Tech, Evolving Terror." CSIS, March 2018.
- Sewell, Kareem Chehayeb, Abby. "Why Protesters in Lebanon Are Taking to the Streets." *Foreign Policy* (blog), 2019.
- Shambhavi Naik. "Biological Weapons: The Impact of New Technologies." *CBW Magazine* (blog), June 2019.
- Sharp, Jeremy M. "Yemen: Civil War and Regional Intervention." *Congressional Research Service*, September 17, 2017, 17.
- Shear, Michael D., Eric Schmitt, Michael Crowley, and Maggie Haberman. "Strikes on Iran Approved by Trump, Then Abruptly Pulled Back." *The New York Times*, June 20, 2019, sec. World.
- Shi Jiangtao. "China, France Sign US\$45 Billion of Deals Including Airbus Order." *South China Morning Post*, March 26, 2019.
- Sico van der Meer, Danny Pronk, and Adája Stoetman. "CBRN Weapons: Where Are We in Averting Armageddon?" Clingendael, November 5, 2019.
- Center for Strategic and International Studies. "Significant Cyber Incidents." Accessed December 9, 2019.
- Silver, Laura, and Christine Huang. "Appendix A: How Smartphone and Social Media Use Relate to Social Network Diversity." *Pew Research Center: Internet, Science & Tech* (blog), August 22, 2019.
- South China Morning Post. "Singapore PM Tells China and US Not to Force Small Nations to Take Sides," June 1, 2019.

- “SIPRI Military Expenditure Database (1949–2018).” SIPRI, September 21, 2019.
- SIPRI. “SIPRI Military Expenditure Database (1949–2018).” Accessed September 12, 2019.
- Slobodian, Natalie. “Political Technologies of Russian Energy Diplomacy.” *Nowa Polityka Wschodnia* 16, no. 1 (March 2018): 49–65.
- Smith, R. Jeffrey. “Hypersonic Missiles Are Unstoppable. And They’re Starting a New Global Arms Race.” *The New York Times*, June 19, 2019, sec. Magazine.
- Smith, Tom W., Michael Davern, Jeremy Freese, and Stephen Morgan. “General Social Surveys, 1972–2018.” National Science Foundation, December 2019.
- Office of the President. “Speech and the Following Discussion at the Munich Conference on Security Policy,” November 29, 2019.
- Spencer Ackerman. “US Officially Accuses Russia of Hacking DNC and Interfering with Election.” *The Guardian*. Accessed November 7, 2019.
- Spiegeleire, Stephan de, Yulia Aleshchenkova, Koen van Lieshout, Christopher Frattina, and Tariq Zaidi. “Nowcasting Geodynamics, Great Powers and Pivoting.” The Hague: The Hague Centre for Strategic Studies, 2017.
- “Splintergroep Binnen WTO Gaat Werken Aan Regels Voor E-Commerce.” *Financieel Dagblad*, January 2019.
- Squire, Megan. “Can Alt-Tech Help the Far Right Build an Alternate Internet?” *Fair Observer* (blog), July 23, 2019.
- Standish, Amy Mackinnon, Reid. “Russians Begin to Consider Life Without Putin.” *Foreign Policy* (blog), 2019.
- President of Russia. “Statement by President of Russia Dmitry Medvedev.” Accessed October 23, 2019.
- Stephan De Spiegeleire, and Tim Sweijs. “The Other Side of the Security Coin.” HCSS, 2017.
- Stephen Krasner. “Structural Causes and Regime Consequences: Regimes as Intervening Variables.” *International Organization*, 1982.
- Steven Andreasen. “Trump Is Quietly Leading Us Closer to Nuclear Disaster.” *Washington Post*, June 2019.

“Strategic Monitor 2018– 2019.” Accessed December 9, 2019.

“Strategy and Work Programme 2007–2008.” ECFR, May 2007.

Stronski, Paul, and Anne Himes. “Russia’s Game in the Balkans,” January 2019.

Sundberg, Ralph, and Erik Melander. “Introducing the UCDP Georeferenced Event Dataset.” *Journal of Peace Research* 50, no. 4 (2013): 523–32.

Sweijjs, Tim, and Floris Holstege. “Threats, Arms and Conflicts: Taking Stock of Interstate Military Competition in Today’s World.” Strategic Monitor 2018–2019. The Hague, Netherlands: The Hague Centre for Strategic Studies, 2019.

Sweijjs, Tim, and Danny Pronk. “Interregnum: Strategic Monitor Annual Report 2019.” The Hague, Netherlands: The Hague Centre for Strategic Studies & The Clingendael Institute, April 2019.

“Syrian Civil War Fast Facts.” *CNN*, October 2019.

Tamma, Paola. “Italy Signs up to China’s Massive Infrastructure Project.” *POLITICO*, March 23, 2019.

Tarmo Virki. “China’s Touchstone to Invest \$17 Billion in Helsinki-Tallinn Tunnel.” *Reuters*, March 8, 2019.

Europol. “Terrorism Evolving: Insights from Research to Combat the Threat,” April 2019.

Europol. “Terrorism Situation and Trend Report 2019,” June 2019.

The Arms Trade Treaty. “The Arms Trade Treaty,” 2018.

The European Parliament and The Council of the European Union. “Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act).” Official Journal of the European Union, April 17, 2019.

The GDELT Project. “The GDELT Project: Data,” 2019.

“The National Security Strategy of the United Kingdom: Update 2009.” Cabinet Office, June 2009.

- “The Secretary General’s Annual Report 2015.” NATO, 2015.
- “The United Arab Emirates in the Horn of Africa.” Middle East Briefing N65. Abu Dhabi: International Crisis Group, November 6, 2018.
- Wassenaar. “The Wassenaar Arrangement.” Accessed September 19, 2019.
- The World Bank Group. “GDP per Capita (Current US\$).” The World Bank Data, 2018.
- Thorington, Kanzanira. “Europe’s Elections: The Fight Against Disinformation.” *Council on Foreign Relations* (blog), May 23, 2019.
- Tim Sweijs, and Danny Pronk. “Interregnum | Strategic Monitor 2018–2019.” HCSS, 2018.
- Timbro Authoritarian Populism Index. “The Data.” Timbro Authoritarian Populism Index 2019, February 2019.
- Torossian, Bianca, Lucas Fagliano, and Tara Görder. “Global Security Pulse October 2019: Hybrid Conflict.” Strategic Monitor Program. The Hague, Netherlands: The Hague Centre for Strategic Studies, October 24, 2019.
- “Treaty on the Non-Proliferation of Nuclear Weapons (NPT).” United Nations Office for Disarmament Affairs (UNODA), 1970.
- Ministry of Foreign Affairs of Japan. “Trends in Chinese Government and Other Vessels in the Waters Surrounding the Senkaku Islands, and Japan’s Response.” Accessed December 9, 2019.
- “Trends in World Military Expenditure, 2018,” April 2019.
- Trevithick, Joseph. “Russia Plans To Launch Tiny Space Plane Off Back Of High Flying M-55 Research Jet.” The Drive. Accessed December 9, 2019.
- Trym Aleksander Eiterjord. “China’s Busy Year in the Arctic,” January 2019.
- “Turkey Justifies Syria Invasion by Claiming Right to Self-Defense under U.N. Charter.” *The Japan Times Online*, October 15, 2019.
- “Turkey’s Downing of Russian Warplane - What We Know.” *BBC News*, December 1, 2015, sec. Middle East.
- UCDP - Uppsala Conflict Data Program. “UCDP - Uppsala Conflict Data Program.” Accessed September 12, 2019.

- Ulfelder, Jay. "Global: More Democracy, Less Freedom." Koto, January 19, 2018.
- UN General Assembly. "United Nations General Assembly Resolution 53/70." United Nations, January 4, 1999.
- UN News. "UN Launches Innovative Programme to Detect and Disrupt Terrorist Travel," May 7, 2019.
- United Nations. "Cyberspace and International Peace and Security - Responding to Complexity in the 21st Century." United Nations Institute for Disarmament Research (UNIDIR), 2017.
- United Nations General Assembly. "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security A/RES/73/266." United Nations, December 22, 2018.
- United Nations Group of Governmental Experts. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/68/98." United Nations General Assembly, June 24, 2013.
- "United Nations Millennium Development Goals." Accessed November 20, 2019.
- United States of America Department of Defense. "Cyber Strategy." U.S. DoD, 2018.
- Unnati Ghia. "International Humanitarian Law In a Post-Truth World." *Cambridge International Law Journal* (blog), December 2018.
- "UNOCT Consolidated Multi-Year Appeal 2019-2020." UNOCT, 2018.
- Urban, Mark. "Salisbury 'shows' Russia Stockpiling Weapons." *BBC News*, March 4, 2019, sec. UK.
- "US Moves Ahead on Nord Stream 2 Sanctions." *EUobserver*, March 2019.
- "US Nuclear Weapons: First Low-Yield Warheads Roll off the Production Line." *The Guardian*, January 28, 2019, sec. World news.
- Van Beek, Ursula, ed. *Democracy Under Threat: A Crisis of Legitimacy?* New York City: Springer, 2018.

Van Manen, Hugo, Amit Arkhipov-Goyal, and Tim Sweijs. “Macro Implications of Micro Transformations: An Assessment of AI’s Impact on Contemporary Geopolitics.” HCSS Security. The Hague, Netherlands: The Hague Centre for Strategic Studies, August 20, 2019.

“Verkenningen Houvast Voor de Krijgsmacht van de Toekomst.” Ministerie van Defensie, 2010.

Vicario, Michela Del, Gianna Vivaldo, Alessandro Bessi, Fabiana Zollo, Antonio Scala, Guido Caldarelli, and Walter Quattrociocchi. “Echo Chambers: Emotional Contagion and Group Polarization on Facebook.” *Scientific Reports* 6, no. 1 (December 1, 2016): 1–12.

VVD, CDA, D66 en ChristenUnie. “Regeerakkoord ‘Vertrouwen in de toekomst’ - Publicatie - Kabinetsformatie.” Bureau Woordvoering Kabinetsformatie, October 10, 2017.

Wakatsuki, Yoko, and Junko Ogura. “Japan: China ‘escalating’ Tensions over Disputed Islands.” CNN. Accessed December 9, 2019.

Walker, Christopher, Jessica Ludwig, Juan Pablo Cardenal, Jacek Hucharczyk, Grigorij Meseznikov, and Gabriela Pleschova. “Sharp Power: Rising Authoritarian Influence.” National Endowment for Democracy and the International Forum for Democratic Studies, May 12, 2017.

Walsh, Eric, and Dave Alexander. “U.S. Slaps Sanctions on Iran Firms after Satellite Launch.” *Reuters*, July 28, 2017.

Warrick. “Use of Weaponized Drones by ISIS Spurs Terrorism Fears.” *The Washington Post*, February 2017.

Waxman, Matthew C. “Cyber Attacks as ‘Force’ under UN Charter Article 2(4).” *International Law Studies* 87, no. 1 (January 1, 2011): 5.

“Weißbuch 2006 Zur Sicherheitspolitik Deutschlands Und Zur Zukunft Der Bundeswehr.” Bundesministerium der Verteidigung, October 2006.

“Weissbuch 2016: Zur Sicherheitspolitik Und Zur Zukunft Der Bundeswehr.” Die Bundesregierung, July 2016.

Welzel, Christian. “WVS 1 to 6 Key Aggregates, Version 1.” Lueneburg, Germany, 2014.

“Wereldwijd Voor Een Veilig Nederland: Geïntegreerde Buitenland- En Veiligheidsstrategie 2018–2022.” The Hague: Ministerie van Buitenlandse Zaken, 2018.

“White Paper 2016: On German Security Policy and the Future of the Bundeswehr.” Federal Ministry of Defense, Germany, June 2016.

Who Said What?: The Security Challenges of Modern Disinformation. Canadian Security Intelligence Service, 2018.

Wike, Richard, Laura Silver, and Alexandra Castillo. “Many People Around the World Are Unhappy With How Democracy Is Working.” *Pew Research Center’s Global Attitudes Project* (blog), April 29, 2019.

Willem Oosterveld, and Bianca Torossian. “A Balancing Act | Strategic Monitor 2018–2019.” HCSS, December 2018.

William Mattessich. “Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting No Physical Damage.” *Columbia Journal of Transnational Law*, August 15, 2016.

Wilson, Audrey. “China Warns Hong Kong After Weekend of Violence.” *Foreign Policy* (blog), 2019.

Wintour, Patrick. “Iran Threatens ‘all-out War’ If Action Taken over Saudi Oil Strike.” *The Guardian*, September 19, 2019, sec. World news.

“WIPO Technology Trends 2019 – Artificial Intelligence,” 2019.

Wood, Graeme. “How Long Can John Bolton Take This?” *The Atlantic*, July 2, 2019.

Working Party on Information Security and Privacy. “The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries.” Organisation for Economic Co-operation and Development, December 16, 2005.

Human Rights Watch. “World Report 2019: Rights Trends in Egypt,” January 17, 2018.

“Xi Jinping Outlines His Vision of ‘Dream and Renaissance.’” *South China Morning Post*, March 18, 2013.

Xu, Ke, Agnes Soucat, Joseph Kutzin, Callum Brindley, Nathalie Vande Maele, Hapsatou Touré, Maria Aranguren Garcia, Dongxue Li, and Helene Barroy. “Public Spending on Health: A Closer Look at Global Trends.” World Health Organisation, 2018.

Yascha Mounk, and Roberto Stefan Foa. “The Signs of Deconsolidation.” *Journal of Democracy*, January 2017.

“Yemen President Calls for UN Action.” *BBC News*, March 25, 2015, sec. Middle East.

Zetter, Kim. “Hacker Lexicon: What Are CNE and CNA?” *WIRED*, June 7, 2016.

“Χίμαιρα: Een Duiding van Het Fenomeen ‘hybride Dreiging.’” *NCTV*, April 2019.



Clingendael

Netherlands Institute of International Relations

In this Strategic Monitor 2019-2020, *Between Order and Chaos? The Writing on the Wall*, we try to decipher the writing on the wall and foresee possible future events and developments that shape the global environment and that affect our national security interests. We conclude that the tenets of the international order continue to shift. Increased global competition goes hand in hand with a persistent erosion of significant aspects of the existing architecture of the international order. Cooperation is giving way to confrontation, and rules are systematically violated while underlying norms are incrementally hollowed out. There are, however, certainly areas in which international cooperation persists, albeit in the context of voluntary and non-binding initiatives of coalitions of the willing, comprising both national and local governments, and increasingly in partnership with non-state and private actors.

Based on our reading of *The Writing on the Wall*, international relations are expected to feature more outright forms of competition in the economic, military, but also in the ideological realm. And the international order is expected to become less liberal in nature and less global in scope, and it will be more fragmented. Now, what does this gloomy outlook mean for the Netherlands? Increasing rivalry between values systems in the world requires that we make more explicit what we stand for, and which way of life we want to protect and develop, and that where possible we actively use our values as an instrument of power and influence in the world of tomorrow.

About the authors

Dr. Tim Sweijts is the Director of Research at *The Hague* Centre for Strategic Studies. He is the initiator, creator, and author of numerous studies, methodologies, and tools for research projects in horizon scanning, conflict analysis, international and national security risk assessment, and strategy and capability development.

Danny Pronk is Senior Research Fellow Strategic Foresight at The Netherlands Institute of International Relations *Clingendael*. His research focuses on security and defense issues, particularly in relation to China and Russia, and on geopolitical trend analysis, alternative futures development, and horizon scanning.

The Hague Centre for Strategic Studies (HCSS) is an independent think tank with a focus on support regarding strategic decision-making, and on advice in the field of international and national security issues.

Clingendael – the Netherlands Institute of International Relations – is a leading think tank and academy on international affairs. Through our analyses, training and public debate we aim to inspire and equip governments, businesses, and civil society in order to contribute to a secure, sustainable and just world.