The Hague Centre for Strategic Studies

HCSS SECURITY

Substantiating the Defence Strategic Challenges

Frank Bekkers, Hans van der Louw, Patrick Bolder and Bianca Torossian

The Hague Centre for Strategic Studies

HCSS helps governments, non-governmental organizations and the private sector to understand the fast-changing environment and seeks to anticipate the challenges of the future with practical policy solutions and advice.

Substantiating the Defence Strategic Challenges

HCSS Security
The Hague Centre for Strategic Studies

Authors: Frank Bekkers, Hans van der Louw, Patrick Bolder and Bianca Torossian

Design: Mihai Eduard Coliban (layout) and Constantin Nimigean (typesetting).

The Hague Centre for Strategic Studies
info@hcss.nl
hcss.nl

Lange Voorhout 1
2514EA
The Hague
The Netherlands

HCSS SECURITY

Substantiating the Defence Strategic Challenges

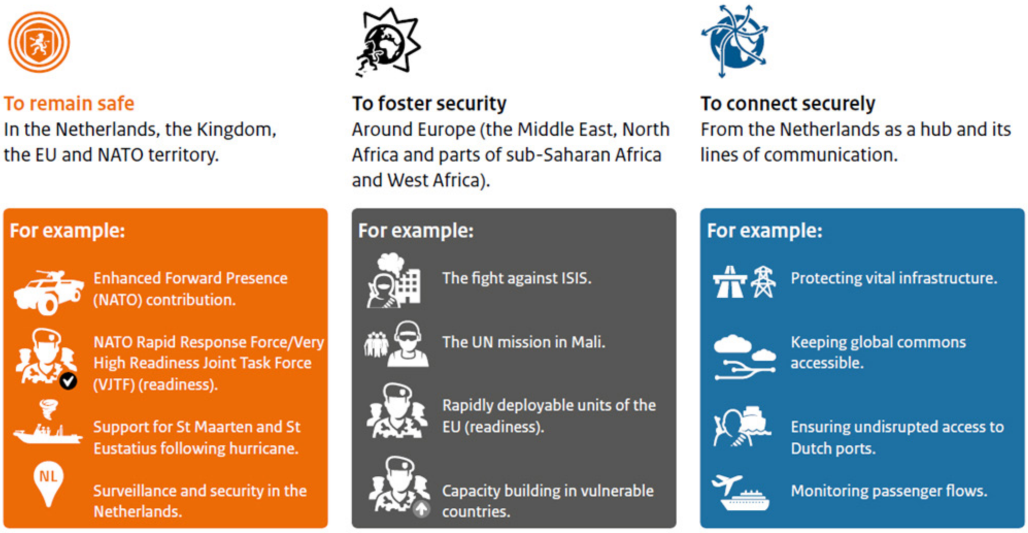
Frank Bekkers, Hans van der Louw, Patrick Bolder and Bianca Torossian

Table of contents

1. Setting the Stage

1.1 Strategic Challenges in a Dynamic Security Environment

Introducing a new perspective. The notion of ‘Strategic Challenges’ for the Netherlands Armed Forces was first introduced in 2017 in a Letter to Parliament: “The three main tasks of Defence and the vital interests included in the International Security Strategy and in the National Security Strategy require Armed Forces with sufficient capacity for action. In view of these main tasks and interests, the Dutch defence effort in the coming years will have to focus primarily on the following three Strategic Challenges.“[1] The 2018 Defence White Paper builds upon this notion, and describes the three Strategic Challenges under the heading “What we want to achieve” as follows: “to **Remain Safe** in the Netherlands, the Kingdom, the EU and the NATO territory; to **Foster Security** in Europe’s neighbouring regions (the Middle East, North Africa and parts of the sub-Saharan Africa and West Africa); to **Secure Connections** from the Netherlands as a hub and its lines of communication”.[2]



To remain safe
In the Netherlands, the Kingdom, the EU and NATO territory.

For example:
- Enhanced Forward Presence (NATO) contribution.
- NATO Rapid Response Force/Very High Readiness Joint Task Force (VJTF) (readiness).
- Support for St Maarten and St Eustatius following hurricane.
- Surveillance and security in the Netherlands.

To foster security
Around Europe (the Middle East, North Africa and parts of sub-Saharan Africa and West Africa).

For example:
- The fight against ISIS.
- The UN mission in Mali.
- Rapidly deployable units of the EU (readiness).
- Capacity building in vulnerable countries.

To connect securely
From the Netherlands as a hub and its lines of communication.

For example:
- Protecting vital infrastructure.
- Keeping global commons accessible.
- Ensuring undisrupted access to Dutch ports.
- Monitoring passenger flows.

Figure 1: Examples of the three Strategic Challenges

[1] Ministry of Defence, Houvast in een onzekere wereld. Lijnen van ontwikkeling in het meerjarig perspectief voor een duurzaam gerede en snel inzetbare krijgsmacht, February 14, 2017, p14.

[2] Ministry of Defence, 2018 Defence White Paper. Investing in our people, capabilities, March 2018, p10.

Why? An important intention behind the introduction of these Strategic Challenges is to provide compelling narratives which are more tangible, more convincing and easier to relate to for a non-expert audience than the - rather 'technical' - main defence tasks. More so than the main tasks, the Strategic Challenges focus on the 'why', rather than on the 'what' and 'how', as the starting point for discussions over the Armed Forces' profile and disposition. However, these narratives have not quite been conceived yet.

Augmenting the main defence tasks with strategic challenges as the core rationale for the existence and basic set-up of the Armed Forces, also offers the opportunity to emphasise the required renewal of the defence organisation. In the period up to 2030-35, the Strategic Challenges - or, more to the point, the possible (military) answers to face these Challenges - will significantly change due to evolving and emerging trends and developments in the security environment. This future-oriented dynamic affecting the characteristics and nature of the Challenges and the associated missions, tasks and force characteristics of the Netherlands Armed Forces stands central in this Study.

Note that the three main defence tasks, as laid down in article 97 of the Constitution of the Kingdom of the Netherlands, remain applicable. Further note that these tasks show considerable overlap with the three Strategic Challenges. The Remain Safe Challenge in effect combines the first and third main defence tasks, Protection of Dutch and NATO territory and Support of civil authorities respectively. The combination of the two acknowledges the fact that national and international security have become largely interwoven. The Foster Security Challenge is equivalent to the second main task, Promotion of the international legal order. The new terminology emphasises the awareness that promoting stability / preventing instability is a key prerequisite for global order. It is the Secure Connections Challenge that is the most innovative of the three, with no direct equivalent in the existing main defence tasks. It embodies the age of globalisation and information, with physical and virtual networks and flows increasingly defining both our economic and societal activities.

Terminology: from Dutch to English

In Dutch, the three Strategic Challenges (*strategische opgaven*) are labelled *Veilig blijven*, *Veiligheid brengen* and *Veilig verbinden*. *Veiligheid* translates to both safety ("the condition of being protected from or unlikely to cause danger, risk, or injury") and security ("the state of being free from danger or threat"). In the context of the tasks of the Armed Forces, the latter is the more appropriate translation. It therefore might be advisable to translate *Veilig blijven* to 'Remain <u>Secure</u>' rather than to 'Remain <u>Safe</u>'. In doing so, the word security / secure / securely consistently returns in all three Challenges. Furthermore, in our minds 'Foster Security' does not fully grasp the essence and intention of

Veiligheid brengen. 'To foster' suggests that security is established and needs to be maintained. In conflict-torn weak and failing states, however, this is not the case; security must be established before it can be 'fostered'. We would therefore suggest 'Provide Security' as the more direct translation of *Veiligheid brengen*.

Throughout this document, we will stick to the terms as introduced in the MoD's translation of the 2018 Defence White Paper. However, in future translations of MoD's policy documents, the above suggestions might be considered.

1.2 This Study

Objective. Applying the lens of the Strategic Challenges to look at the security environment and the role of the Netherlands therein, has consequences for the types of missions and tasks[3] the Armed Forces must be capable of, and thus for the (future) military capability portfolio. The objective of this Study is to add (1) future-oriented elements to further substantiate the narrative for each of the Strategic Challenges; and thereby (2) to link (the dynamics within) the Strategic Challenges to (future) missions for the Armed Forces and associated defence capability portfolio choices. These results can be used within the context of the next Defence White Paper (presumably labelled as a 'vision' with a 10-15-year time horizon), scheduled for publication in the first half of 2020.

This document has the following structure. In Chapter 2 we provide some general guidance to the Strategic Challenges storylines by summarising the strategic goals of security and defence policy; the evolving world order; and the general trends and developments that are likely to affect the global security environment in terms of both risks and opportunities. Chapters 3, 4 and 5 give substance to each of the three Strategic Challenges, concentrating on 'new' elements that are, in our opinion, under-appreciated in the current mainstream defence debate. The issues raised stem from an 'outside-in' perspective on how the dynamic security environment affects the missions and tasks, partners, operating concepts, and high-level force characteristics of the Netherlands Armed Forces. Lastly, in Chapter 6 we look at some of the key synergistic elements transcending the individual Strategic Challenges, shaping the overall layout and performance of the Armed Forces.

[3] In this document, (military) tasks are defined as specific actions that must be performed in order to accomplish a military operational objective. Tasks may be expressed at various abstraction levels. An example is the high-level categorisation used by NATO: prepare, project, engage, protect, sustain, inform, consult and command & control. In a (military) mission or operation, a mix of tasks is applied in a real-world setting (as defined by the threat, environment, coalition etc.). Note that the three main tasks do not qualify as tasks in this sense, because they are phrased in terms of political and strategic objectives, rather than military operational ones. 'Strategic Challenges' is a more apt phrasing than 'main tasks' to cover the high-level objectives set for the Armed Forces.

2. A Structuring Framework

In order to substantiate the narrative for each of the three Strategic Challenges, it is imperative to have a clear understanding of the political and military objectives the Netherlands would like to see achieved under each of the Challenges; and of the essential characteristics that clearly differentiate the Challenges, as well as the elements that bind them in the overall role of the Armed Forces as a distinct and important societal institution. However, the 2018 Defence White Paper provides little specifics on these qualities. In this Chapter, we therefore turn to the Integrated International Security Strategy for 2018 to 2022 (2018 IISS)[4] and the 2019 National Security Strategy (2019 NSS)[5] for initial guidance. These two policy documents elaborate the strategic objectives of Dutch security policy in more detail than the Defence White Paper.

In addition, we provide a short overview of key trends in the security environment that will influence both the Strategic Challenges and the way the Armed Forces may meet these Challenges; and suggest a high-level Framework to assess the strategic impact of these trends.

2.1 Strategic Objectives for Security and Defence

2018 IISS. The Integrated International Security Strategy defines three pillars substantiating such a strategy: Prevent, Defend and Strengthen. The Netherlands' strategic efforts are guided by thirteen **Strategic Goals** associated with the three pillars, as shown in Figure 2.

2019 NSS. Whereas the IISS largely uses verbs to describe the three pillars and underlying Strategic Goals, the National Security Strategy uses nouns to define the **Vital Interests** of the Kingdom (see text box below). These Vital Interests pertain to 1. territorial security; 2. economic security; 3. ecological security; 4. physical security; 5. social and political stability; and 6. (the functioning of) the international legal order.[6] National security

[4] Ministry of Foreign Affairs, Working Worldwide for the Security of the Netherlands. An Integrated International Security Strategy 2018-2022, March 2018.

[5] Ministry of Justice and Security, Nationale Veiligheid Strategie 2019, 7 June 2019.

[6] Since the publication of the first iteration of the NSS in 2007, the categorisation of national interests has been remarkably stable. In the 2019 NSS, (the functioning of) the international legal order was added to reflect the fact that the Netherlands is increasingly dependent on a functioning system of international standards and agreements for the realisation of its national security.

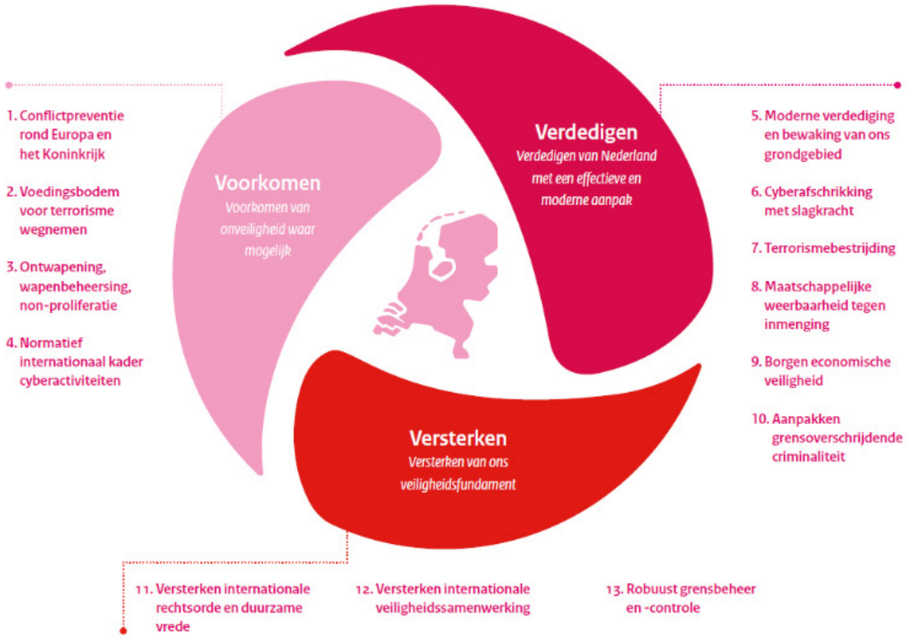

1. Conflictpreventie rond Europa en het Koninkrijk
2. Voedingsbodem voor terrorisme wegnemen
3. Ontwapening, wapenbeheersing, non-proliferatie
4. Normatief internationaal kader cyberactiviteiten
Voorkomen
Voorkomen van onveiligheid waar mogelijk
Verdedigen
Verdedigen van Nederland met een effectieve en moderne aanpak
5. Moderne verdediging en bewaking van ons grondgebied
6. Cyberafschrikking met slagkracht
7. Terrorismebestrijding
8. Maatschappelijke weerbaarheid tegen inmenging
9. Borgen economische veiligheid
10. Aanpakken grensoverschrijdende criminaliteit
Versterken
Versterken van ons veiligheidsfundament
11. Versterken internationale rechtsorde en duurzame vrede
12. Versterken internationale veiligheidssamenwerking
13. Robuust grensbeheer en -controle

Figure 2: 2018 IISS' Strategic Goals

is at stake when one or more national security interests are threatened in a way that societal disruption may occur. In particular, security interests 1., 2. and 5. could be challenged both physically and through digital space. The availability, confidentiality, and integrity of essential information services are added with the 2019 NSS as criteria for territorial security and are consequently an element of our national security.

Verbs and nouns

By using verbs, the Strategic Goals of the 2018 IISS are more action-oriented, but also more time sensitive than the Vital Interests of the 2019 NSS, which denote enduring values, stakes and concerns that remain relatively stable over time. Indeed, essentially the same concepts can be expressed in abstractions of thinking and precise definitions separated from day to day practices (through nouns) as well as in terms of actual practices that are part of unfolding configurations (through verbs). Both approaches have merit and should be seen as complementary, reflecting the dual nature of strategic processes, where on the one hand one attempts to impose concepts on an environment in an attempt to mould or control processes, while on the other hand acknowledging the fact that concepts are part of constantly changing configurations, and should therefore be flexible and inherently responsive to environmental changes.

Defence White Paper. In the 2018 Defence White Paper, three **Strategic Challenges** were defined: Remain Safe, Foster Security and Secure Connections. These Strategic Challenges are clearly presented as separate efforts but should at the same time be considered as interlinked and overlapping. The integral nature of the Challenges is reflected in the fact that, except for some relatively minor assets, the Dutch Armed Forces do not have dedicated, separate capability toolboxes for each of the Challenges and the associated missions and tasks. Indeed, having an integrated toolbox capable of conducting a wide range of missions and tasks across the three Strategic Challenges is seen as a critical design feature for a flexible, yet robust force able to face a highly dynamic security environment that (re)presents a wide variety of potential risks and threats.

An integrated security strategy?

The Netherlands, with its tradition of highly autonomous ministries, has no overarching 'grand strategy' for its security and defence posture. In its 2017 coalition agreement, the government promised to formulate "a security strategy that addresses domestic and foreign threats, including terrorism, and which replaces the current International Security Strategy".[7] The *Wetenschappelijke Raad voor het Regeringsbeleid* does the same.[8] Although the 2018 IISS claims to be this overarching strategy,[9] it isn't. And while the 2018 Defence White Paper and the 2018 IISS refer to one another, and the 2019 NSS refers to the 2018 IISS (the 2018 IISS does not refer to the 2019 NSS), this does not imply a coherent government-wide strategic framework. All documents have their own creation process and framework, with the cross-references largely paying lip service to an integrated approach, rather than actually stemming from such an approach.

In an arena where international and national and military and non-military security challenges increasingly merge; crime, terrorism and cyberattacks defy borders; grey zone conflicts are upon us; and a growing consensus emerges that a whole of government and, indeed, a whole of society approach to security is required, this must change. We believe that our country needs a truly Integrated Security Strategy, anchored in an explicitly related, partly hierarchical, partly dovetailed network of strategic policy documents such as (regularly updated versions of) the IISS, the NSS and the Defence White Paper. This paper trail is not an end in itself, but is required to provide high-level guidance for priority, tasking and capability choices for the various agencies that contribute to Dutch resilience in the face of a wide variety of security challenges.

[7] Vertrouwen in de toekomst. Regeerakkoord 2017 – 2021, 2017, p48.

[8] "The WRR advises to develop the future of the Armed Forces based on an integrated security strategy that includes internal and external security." WRR, Veiligheid in een wereld van verbindingen. Een Strategische Visie op het Defensiebeleid, 2017, p10.

[9] 2018 IISS, p6.

Relationship. Table 1 shows how the Strategic Goals of the 2018 IISS and the Vital Interests of the 2019 NSS map according to the Strategic Challenges. Because each set has its own rationale, the details of this mapping exercise are open to interpretation and debate. However, since this mapping only serves as an initial starting point to provide a better sense of purpose for each of the Strategic Challenges - a sense that is largely missing in the 2018 Defence White Paper - we present this mapping as-is and refrain from further elaboration.

Strategic Challenge	Associated IISS goals	Associated NSS interests
Remain Safe	3. Disarmament, arms control and non-proliferation of weapons of mass destruction	1. Territorial security
	5. Modern collective self-defence and protection of Dutch and NATO territory	1. Territorial security
	6. Forceful cyber deterrence	1. Territorial security 4. Physical security
	7. Counterterrorism	4. Physical security 5. Social and political stability
	8. Societal resilience to foreign interference	5. Social and political stability
	9. Safeguarding economic security	2. Economic security
	10. Tackling cross-border crime	4. Physical security 5. Social and political stability
	12. Strengthening international security cooperation	1. Territorial security 2. Economic security 3. Ecological security[10]
Foster Security	1. Preventing conflict around Europe and the Kingdom	4. Physical security 5. Social and political stability
	2. Eliminating the root causes of terrorism	4. Physical security 5. Social and political stability
	3. Disarmament, arms control and non-proliferation of weapons of mass destruction	6. International legal order
	10. Tackling cross-border crime	6. International legal order
	11. Promoting the international legal order	6. International legal order
	12. Strengthening international security cooperation	3. Ecological security 6. International legal order

[10] The 2018 IISS refers to the Sustainable Development Goals as the ultimate prevention agenda, addressing the root causes of instability and conflict. Goal 1 of the 2018 IISS, Preventing conflict around Europe and the Kingdom, mentions the *effects* of climate change as one of the drivers of instability and crises that warrants preventive actions. However, ecological security as such is not directly represented in the Strategic Goals.

Strategic Challenge	Associated IISS goals	Associated NSS interests
Secure Connections	4. Clear international norms for cyber activities	2. Economic security
	6. Forceful cyber deterrence	2. Economic security
	9. Safeguarding economic security	2. Economic security
	10. Tackling cross-border crime	2. Economic security
	11. Promoting the international legal order	2. Economic security
	12. Strengthening international security cooperation	2. Economic security
	13. Robust and balanced integrated border management and control	2. Economic security

Table 1: Mapping of the 2018 IISS Strategic Goals and 2019 NSS Vital Interest on the Defence White Paper Strategic Challenges

2.2 Future Worlds

'Future worlds' Framework. The substantive Chapters 15 through 0 are future-oriented, with a time horizon of 10-15 years into the future. In order to capture some of the fundamental uncertainties of how the future will unfold, we use the Framework first introduced in the MoD's 2010 Future Policy Survey.[11] This Framework facilitates first order thinking about how the three Challenges and associated missions, tasks and force characteristics may evolve in the period up to 2030-35. It proposes two core uncertainties that determine the geopolitical security environment: the relative power of state versus non-state actors and the level of cooperation between key actors. Using these two core uncertainties as axes in a diagram, four distinct world views may be discerned.[12]

Netherlands' ambitions in terms of this Framework. In general terms, the Netherlands strives for a cooperative world based on a world order that provides a level playing field for smaller nations such as the Netherlands; an order underpinned and, if and when needed, enforced by global institutions and international laws, regulations and treaties. At the same time, the Netherlands hedges against a less benign world where diverging interests may lead to escalating conflict—and contributes to the prevention of such conflict happening. In other words, the Netherlands actively promotes a world order that corresponds with the right-hand side of the Framework, while acknowledging that movements towards the left may occur in practice - as is indeed visible over the past couple of years - and require mitigating policy.

[11] Ministry of Defence, *Future Policy Survey. A new foundation for the Netherlands Armed Forces*, 2010.

[12] We prefer the term 'world views' over the term 'scenarios' as used by the Future Policy Survey.

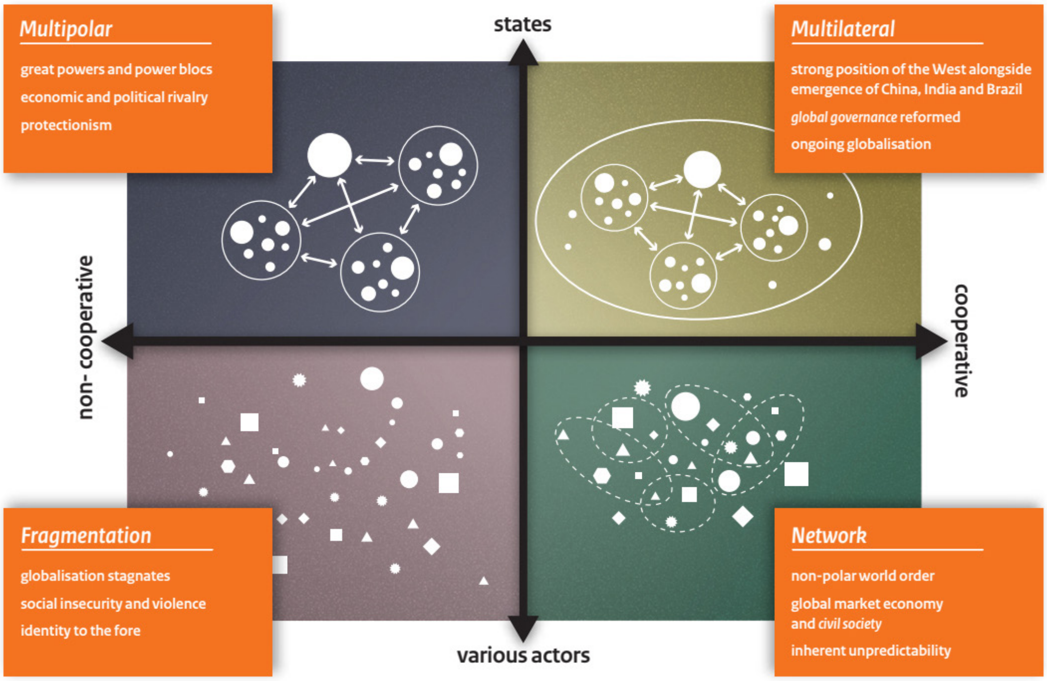

Multipolar
great powers and power blocs
economic and political rivalry
protectionism
states
Multilateral
strong position of the West alongside emergence of China, India and Brazil
global governance reformed
ongoing globalisation
non- cooperative
cooperative
Fragmentation
globalisation stagnates
social insecurity and violence
identity to the fore
various actors
Network
non-polar world order
global market economy and civil society
inherent unpredictability

Figure 3: Framework to discern four distinct world views[13]

Dutch policy is further built upon the presumption that states remain the principal agents for maintaining international order and stability, but increasingly interact with non-state actors such as NGOs, international corporations and other societal partners to do so. In terms of the Framework, over time an evolution downwards is anticipated: state power, whilst remaining the single most relevant factor in shaping global order for the foreseeable future, gradually diminishes relative to power exerted by a wide array of non-state actors in the international arena. The Netherlands actively supports a policy of increasing engagement with many of these non-state actors in pursuing and safeguarding national interests.

A multi-order world. The 'Future Worlds' Framework is a simplified model of the real world. In fact, the international system is characterised by a multi-order rather than by one order, with actors cooperating on specific themes within changing coalitions.[14] As a sum-total trend, however, international cooperation is declining. Over the past five years or so, in most of the various areas of international interaction a tendency away from cooperation towards conflict is visible, accompanied by the systematic violation of international rules and norms. In the years ahead, this shift to the left in the

[13] Note that the 2010 Future Policy Survey incorrectly labels the upper left-hand quadrant. calls this quadrant 'Multipolar'. This is not a defining distinction: all other quadrants are also characterised by multipolarity for the foreseeable future. We propose to change this label into 'Polarisation'. Polarisation is a state wherein multiple (mainly state) actors, to varying degrees and possibly in changing configurations, clash over (real or perceived) mutually exclusive vital interests. This is consistent with the verbiage used in the Strategic Monitor (HCSS and Clingendael, *Interregnum. Strategic Monitor 2018-2019*, March 2019).

[14] HCSS & Clingendael, Stilte voor de Storm? Strategische Monitor 2017-2018, February 2018.

Framework is expected to consolidate and even worsen rather than reverse. Still, even as the multilateral world order is waning, there is as of yet no new, dominant type of order. The end of the post-war multilateral world order based on cooperation and rules has been loudly proclaimed in recent years. And yet there is no robust evidence for it.

A period of transition. In short, as the Strategic Monitor puts it, there is an interregnum. The international system is undergoing a phase transition between different system states, and it is unclear when the system will settle again and in what state that will be. In the meantime, the transition phase is characterised by unusual dynamics and events.[15] Some crucial elements of the current geopolitical era are:[16]

- States are applying a narrower interpretation of self-interest, with a growing prevalence of zero-sum thinking. The discourse is harshening both nationally and internationally. Assertive and even aggressive use of language, that would have been out of character among political leaders two generations ago, is increasingly seen as normal and commonplace.
- In key areas such as peace and security, military competition, arms control, free trade and climate policy, international cooperation is weakening, and conflictive tendencies are rising.
- Freedom is declining in societies in various regions around the world. With no dominant new principles of order replacing the old, the rise of China in particular is accompanied by the formation of new regimes whose governments play a more central role and in which there is less focus on the rights of the individual.
- There is also increasing division within societies. This is usually linked to confusion and uncertainty among citizens about the future. This fuels vertical tensions that then impact international cooperation, within Europe and outside. The acceptance, deepening and dissemination of liberal-secular values can no longer be taken for granted – either globally or in the West.
- On the other hand, a number of basic elements of the international order system still apply. Nation states continue to enter into agreements amid developments in the international legal order, and thus continue to codify prevailing norms into rules.
- This is increasingly done in cooperation with non-state and sub-state actors. International forums increasingly act as hubs providing vital mechanisms to regulate and coordinate state interaction and policy.
- Despite tensions within the EU and NATO on key themes, these organisations that are central to the Netherlands are by no means moribund. At the same time, political worries about the unity of NATO and the EU, as well as their collective defence commitments, will shift the emphasis to coalitions of the willing with like-minded countries.

[15] HCSS & Clingendael, Interregnum. Strategic Monitor 2018-2019, March 27, 2019.

[16] Largely based on Ibid, p35-36.

2.3 Trends and Developments

Systemic trends. In Table 2 below, we list several trends and developments important for the evolution of the Strategic Challenges. This table serves as a stepping stone to Strategic Challenge specific elaborations in Chapters 3 through 5. The above discussion on the level of global cooperation and the power balance between state and non-state actors is reflected in this list.

Geopolitical Context	
Great power rivalry	We see a growing competition between great powers and power blocks, with escalating potential and an increase of proxy wars. Emerging powers are challenging traditional powers over resources, territory and influence. Russia uses hybrid tactics to pursue its aims at the borders of Europe. China's Belt and Road Initiative has distinct political dimensions with, ultimately, regional and global military implications. In the Indo-Pacific region, China's military ambitions are growing, directly challenging the US and, indirectly, its Allies. A new arms race, also in nuclear terms, is manifesting itself.
Intra-state conflict	Growing inequality, mass unemployment and societal fragmentation, exacerbated by social media, increase the risk of intra-state and non-state conflict. Furthermore, the number of intra-state conflicts with external countries intervening has increased. These conflicts tend to last longer and become more violent. Intra-state conflicts may create ungoverned spaces that serve as breeding grounds, safe havens and launching platforms for e.g. (the nexus of) international terrorism and international crime.
Climate change	Climate change acts as both a threat instigator and multiplier.[17] Migration flows, humanitarian crises and associated security issues that are rooted in or are amplified by the effects of climate change, may multiply over the period up to 2030-35 (and beyond).
Approaches and arenas	
Hybrid/grey zone conflict[18]	Grey zone conflict is likely to become more frequent; and is already upon us (the 'west'). Hybrid warfare is likely to be a pervasive feature of future conflict. A key feature of hybrid tactics is using misinformation (fake news) through social media channels, discrediting information flows. The information domain is an important new arena for conflict and (therefore) for military actions.
The global commons	As reliance on the global commons increases, maintaining freedom of access will be a vital objective for governments. Cyberspace and space are quickly becoming a vital part of the global commons. Cyberspace is already an active battleground, with state and non-state actors continuously searching for adversaries' vulnerabilities, trying to obtain secret information, developing cyber weapons and occasionally deploying them. China and Russia, with other autocracies following suit, are building their own segment of the internet — a kind of digital A2AD environment — thereby reducing their cyber (and information) vulnerability and threatening the notion of the internet as a public good. Furthermore, the space domain is becoming increasingly militarised.
Urban conflict	As more and more people opt to live in (large) cities, these virtual and physical hubs generate the vast majority of economic activities and act as nuclei of information flows. Armed Forces face a dilemma: they prefer to stay away from the complex urban environment but realise that the key factors where conflicts are fought over increasingly reside there.

[17] Ministry of Defence, Future Policy Survey. A new foundation for the Netherlands Armed Forces, 2010, p81-82.

[18] See textbox on page 18 for a discussion on terminology.

Actors	
Non-state actors	An increasing number of non-state actors may drive conflict or pose security challenges, e.g. corporations seeking resources, large numbers of disenfranchised or excluded citizens causing civil conflict, criminal organisations exploiting cyberspace. Non-state actors may also seek to influence groups in society and the larger public: inspire terrorism, instigate public protest (e.g. the yellow vest movement).
Multi-domain (military) operations	The mutual relationships between the domains of land, sea, air, space, electromagnetic spectrum, cyber and information increase with the operational distinctions fading. Multi-domain and multi-level joint military operations need to be brought to the next level (within a WoG/WoS context, see below).
Whole of Government approaches	Both attackers and defenders in hybrid engagements synchronise their diplomatic (or political), informational, military, economic and legal (DIMEL) state instruments of power to vertically and horizontally escalate a series of specific activities in order to achieve effects.
Whole of Society approaches	In an era where violent security threats are no longer only issued by and no longer only aimed at states and state institutions, societal resilience is of increasing importance. Defence might expand its role in building and supporting societal resilience, both in the Netherlands and possibly in potential conflict regions in the periphery of Europe. Defence organisations that can best manage their (national) ecosystems with private industry, especially with technology firms, are likely to derive a crucial advantage in future conflicts.
Technology and Capabilities	
Developments in weapon technology	Nuclear weapons: Tactical nuclear weapons likely lead to a higher risk that nuclear weapons will be employed in inter-state conflict, especially now that there seems little appetite for updating or renewing ending arms treaties. Chemical and biological weapons: Developments in biology and chemistry could make BC-weapons more attractive to potential users. Precision strike: Advanced hypersonic stand-off weapons make distance increasingly irrelevant as a security buffer or defence. Swarm technology: Accelerating improvements in robotics, artificial intelligence, additive manufacturing (3D printing) and nano-energetics are dramatically changing the character of conflict in all domains. Small, smart and cheap weapons based on the convergence of these technologies may be able to dominate combat. These capabilities become available not just to major powers, but to smaller and smaller agents — extending even to the individual. “Because even massive investment in mature technology leads to only incremental improvement in capabilities, the proliferation of many small and smart weapons may simply overwhelm a few exceptionally capable and complex systems.”[19] This diffusion of power will greatly complicate responses to various crises, reduces the ability of Western alliances to influence events with military force, and requires policymakers and military planners to thoughtfully consider procurement plans, force structure and force posture.
Proliferation of weapon technology	Cheap, readily available equipment - such as cyberattack tools, weaponised drones and bio-engineered viruses allow, for example, violent extremist organisations or even individuals, to cause heavy financial, societal, and human losses at a relatively low cost to themselves.

[19] T. X. Hammes, Technologies Converge and Power Diffuses. The Evolution of Small, Smart, and Cheap Weapons, January 2016.

Technology and Capabilities (cont.)	
Technological dependence	Defence organisations have increasingly become dependent on enabling technologies and standards that are developed in and enforced by global civil markets. This applies to (underlying technologies for) ICT, sensors, energy supply, mobility and logistics solutions and much more. Defence organisations are becoming increasingly dependent on those companies that create and 'own' these technologies and standards (through IPR or market dominance). Even when doing business with familiar system integrators, the underlying supply chains at the lower tiers are almost invariably dependent on the international market and/or are not fully transparent. In particular, the dependency of military supply chains on China is large and worrisome.[20] For example, China seeks to dominate 5G standard-setting and patent rights as part of a broader strategy of global technology dominance.
AI in the OODA loop	Actors with the best sensors, data and algorithms will achieve an important competitive advantage. AI will have huge consequences for military decision-making, especially if humans are removed from the various decision loops. China is leading in the field of AI, with the strategic and political culture in China more tolerant to an early adaptation to AI-powered autonomous decision-making. This could greatly enhance the effectiveness of, for example, its A2AD systems. Other autocracies, including Russia, tend to have a similar position on this issue.

Table 2: Trends and developments that might affect the dynamics in the Strategic Challenges

[20] U.S. Department of Defense, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States.

3. Dynamics in To Remain Safe

In this Chapter, we describe some of the more salient, but possibly currently underexposed, developments that drive innovation in the Remain Safe Challenge for the period up to 2030-35.

3.1 Defence as an Integral Part of Contemporary Society

Geo-political competition as a defining characteristic of the age. To Remain Safe is the most urgent challenge in a world with little cooperation and therefore much potential for (violent) conflict that may indirectly, directly or even existentially threaten Dutch vital interests - i.e. the left-hand side of the 'Future Worlds' Framework in Chapter 2. As previously described, in recent years we have observed a clear trend towards a more competitive global order. With an ongoing power shift from 'West' to 'East' and an ever-higher demand on scarce resources from a growing global consumer class, states and other actors will more assertively and even aggressively put their own interests first. Many states show an increased willingness to use military power, or the threat thereof, to support their political and economic interests.[21] Sometimes, these interests are value-based and/or identity-driven - or disguised as such.[22] This is *not* to say that the next 10-15 years will necessarily see a 'zero-sum' world emerging, with great powers in a perpetual state of conflict because one's loss is another's gain. On many issues, the international order still functions, with major pundits acting according to their responsibility for the common good (win-win approach) - with currently China increasingly cooperating whilst the US is engaging less with other states on global challenges such as climate change.

First and third main defence tasks merge. For two decades, the fact that national and international security issues increasingly interact and overlap has been discussed by security experts. But only with the MH17 incident (see text box below), the notion that seemingly distant threats may affect Dutch society directly really entered the Dutch public debate. Today, it is broadly understood that security of and within Dutch society is intrinsically linked with manifestations of globalisation and of an increased global power competition. Hybrid confrontations, international terrorism

[21] Ministry of Defence, Houvast in een onzekere wereld. Lijnen van ontwikkeling in het meerjarig perspectief voor een duurzaam gerede en snel inzetbare krijgsmacht, February 14, 2017, p5.

[22] Ibid, p6.

and the security effects of large migration flows, to name some highly visible issues in the international arena, require an increased resilience of Dutch society. As a result, the first and third main defence tasks - Protection of Dutch and NATO territory and Support of civil authorities respectively - tend to merge within the context of the Remain Safe Challenge; and change character because of it.

MH17 as a wake-up call

On 17 July 2014, Malaysia Airlines flight MH17 crashed in the fields of eastern Ukraine, after being hit by a Russian-made missile. 298 people lost their lives, 196 of them Dutch. For the Netherlands, the downing of flight MH17 and the aftermath served as a wake-up call. It showed not only how a non-frontline state could be directly hit by tensions at the periphery of Europe, but also how Dutch society could become the target for a modern disinformation campaign. The downing of MH17 also marked a Rubicon moment for the Russian disinformation machine: it was the first time that the full power of the state was trained on convincing the world to accept a false narrative of events, despite a preponderance of evidence to the contrary. Internet trolls, hackers, Kremlin-run media such as RT and Sputnik, retired soldiers, public officials and anonymous programmers combined forces to achieve a common goal: the discrediting of all those who claimed that Russia had some part in the missile attack.

Defence as a basic and visible societal function. A crucial notion in the Remain Safe narrative is therefore that defence, both the activity and the organisation, have (once again) become an integral part of society; with both society and the armed forces still in the process of internalising and adapting to this fact. In other words, the notion of the Armed Forces as something distinct from the day-to-day lives of citizens, the combination of an insurance policy kept in a closed drawer (i.e. gated barracks in thinly populated rural areas)[23] and a foreign policy tool mainly deployed in far-away places, is completely outdated. The defence organisation should more forcefully adapt to this new reality, claiming more visibility in the national security debate. As a key instrument of state power[24], the military could boost its - currently largely latent - role in e.g. critical infrastructure protection and in strengthening societal resilience against security threats. Senior officers have the right, and the duty, to be vocal about their professional perspective on the security risks and threats

[23] All major military bases are located outside the Randstad in e.g. Den Helder, Oirschot, Havelte, Volkel and Leeuwarden. The projected new Marines base in Vlissingen can be added to the list. The Armed Forces have almost completely vacated their foothold in Amsterdam, the Capital and largest city of the country. This situation does not agree with the regained position of defence as an integral part of society, and should preferably be reversed.

[24] Literature typically refers to Diplomatic (or political), Informational, Military, Economic (including financial) and Legal (DIMEL) instruments a State may utilise to protect its national interests.

our country faces.[25] Furthermore, because today's complex security challenges require a multidisciplinary approach, the military must actively engage with a host of possible partners in an emerging 'security ecosystem' that spans society. This runs against the grain of an organisation that traditionally has a closed personnel system,[26] strives to be self-supporting and prefers to do business with international military peers, but is a key element of the cultural change the MoD has to go through towards "an adaptive force".[27]

Focus on 'security/defence at home'. With the rapidly waning ability of the West to shape global affairs, homeland defence, in the wider sense of both the Netherlands and Europe, has unmistakably become the focus of the Remain Safe Challenge. This shift of focus from the past two decades, in which out of area operations were the norm, requires rethinking the basics of the layout, composition and operating modes of the Armed Forces. The next Sections elaborate aspects of this (regained) focus.

3.2 Conflicts likely to play out in the 'grey zone'

A comprehensive hybrid strategy urgently required. The grown antagonism between major pundits manifests itself in what we call sub-threshold, grey zone or hybrid conflict (see text box below). Russia seems constantly engaged in hybrid operations to test the strengths and weaknesses, the political resolve and societal resilience - or lack thereof - of NATO, the EU and their Member States. In the Russian mindset, this is more than just tactics. Hybrid actions have a strategic objective in providing valuable intelligence and shaping the battlespace for potential future hot conflicts. If escalation to open war does take place, this typically would be a 'war of necessity' rather than a 'war of choice'. In a war of necessity vital national interests are at stake and, as important, viable alternatives to the use of force to protect these interests are lacking. A crucial observation is that, with Western dominance declined and further eroding, we (the Netherlands, Europe, the West) must seek our own hybrid strategies that are active as part of one's own strategy next to reactive in order to counter opponents' hybrid strategy. The capabilities and political will to conduct hybrid actions are an important element of modern cross-domain deterrence and must be further developed, in accordance with western (legal and ethical) standards.[28] [29]

[25] The way high-ranking military officers in the U.S. engage in national security debates, and indeed become politically active or take on government positions after their military career, serves as an illustration.

[26] Alternatives may include horizontal entrance of (new) personnel and (more) exchanges with other government services and with private industry.

[27] https://www.defensie.nl/actueel/nieuws/2017/01/13/defensie-flexibeler-met-de-adaptieve-krijgsmacht

[28] Cf. the Russian concept of 'strategic deterrence'. According to the 2015 Russian National Security Strategy "interrelated political, military, military technical, diplomatic, economic, informational, and other measures are being developed and implemented in order to ensure strategic deterrence and the prevention of armed conflicts. These measures are intended to prevent the use of armed force against Russia, and to protect its sovereignty and territorial integrity.", http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf.

[29] Rob de Wijk, *The Role of Deterrence in a new European strategic environment*, 2018, https://www.degruyter.com/view/j/sirius.2018.2.issue-1/sirius-2018-0023/sirius-2018-0023.xml.

Grey zone conflicts and hybrid threats / conflicts / war

We here use the terms grey zone conflict, hybrid threats and hybrid conflict largely interchangeably. In grey zone or hybrid conflicts, states conduct activities to gradually, but fundamentally, revise the regional or global system of alliances and international norms. 'Grey zone' emphasises that these activities are prolonged and take place in the grey zone between peace, conflict and war - i.e. are not necessarily violent and may only occasionally pass the threshold of war. Furthermore, the 'point of victory' is highly ambiguous. 'Hybrid' points to the wide range of overt and covert military, paramilitary and civilian measures employed in an integrated design. This approach may continue even when conflict evolves into warlike scenarios: non-military actors and stakeholders are then explicitly involved in the political, informational and economic components of war. The degree of reliance on civilians and non-state actors makes hybrid warfare distinctly modern.[30] Hybrid warfare is no longer just about partisans such as the French resistance during the Second World War, but societal in scope in terms of intended targets and the actors that engage in it.

It is important to realise that hybrid / grey zone strategies carry significant potential costs and limitations. They don't escape basic strategic dilemmas. Even if they remain under certain thresholds that would trigger escalatory responses, they tend to generate balancing behaviour that cancels out a significant proportion of their intended results. In practice, grey zone aggression *does* mark its authors as threatening and operating outside the bounds of acceptable behaviour in the context of international rules, norms and institutions. The limitations of hybrid campaigns mean that an effective response can be mounted.

Countering hybrid threats a national responsibility. NATO states that the primary responsibility to respond to hybrid threats or attacks rests with the targeted nation.[31] The EU has a similar approach. For the Netherlands' Armed Forces, this implies that

[30] Although in mainstream discourse the term 'hybrid warfare' has been used with some elasticity to (also) denote hybrid activities in the grey zone, the original concept is to describe the changing character of warfare against violent adversaries during armed conflict. See the discussion on the difference between hybrid threats and hybrid warfare in MCCC Countering Hybrid Warfare Project, *Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces. Conceptual Note*, March 2019.

[31] NATO has set up counter-hybrid support teams to provide assistance to Allies upon request. NATO has further strengthened its coordination with the EU in countering hybrid threats, among others by establishing the European Centre of Excellence for Countering Hybrid Threats (located in Helsinki, Finland), which serves as a hub of expertise, assisting participating countries in improving their civil-military capabilities, resilience and preparedness to counter hybrid threats. Other relevant CoEs include the Strategic Communications Centre of Excellence in Riga, Latvia; the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia; and the Energy Security Centre of Excellence in Vilnius, Lithuania. Note that all these CoEs are in countries on NATO's eastern flank, bordering with Russia.

capabilities need to be better tailored to a national response, in close coordination with other relevant government organisations and with society at large (in §0 we will discuss the concept of resilience and the Whole of Government/Society approach towards it). Hybrid/grey zone activities are an astute object for concept development, as they "creep up on their goals gradually",[32] rather than involving decisive moves. To conceptually and operationally develop effective responses is a critical challenge for the Netherlands / Europe / the West for the coming years. The Armed Forces should be an important driving force behind this. The intellectual capacity for doing so must be strengthened, in the organisation itself as well as within the external ecosystem of strategic knowledge partners.

Adapting the military authority and toolbox to 'security/defence at home'. Since 2005, the Ministry of Defence has strived for increased cooperation with civil authorities beyond a 'safety net' construction.[33] These discussions must be revived, but with a twist. In this age of grey zone conflicts and hybrid threats that unfold domestically, the legal and socially acceptable role of the military needs to be re-gauged. We – Dutch government and Dutch society as a whole - must find intermediate positions between the military fully operating under the authority and in support of civil authorities, with little independent room to manoeuvre; and largely autonomous military operations with little civil oversight, with the potential of an erosion of democratic structures and norms (e.g. because the military instrument is not set to properly discriminate between enablers and the more disengaged).

Furthermore, in most 'security at home' scenarios, the coarser forms of physical violence that our Armed Forces routinely apply in operations abroad, would never be allowed.[34] More discretionary, fit-for-purpose and subtle forms of violence and nonviolent influencing operations, especially in our urban environments (this is expanded upon in §4.3), are required.[35]

3.3 National Sovereignty and International Cooperation

Freedom of action to protect vital interests. The protection of Dutch sovereignty is a Constitutional task. Article 3.1(a) of the Charter for the Kingdom of the

[32] Michael J. Mazarr, Mastering the gray zone: understanding a changing era of conflict, December 2015.

[33] Subsequently under the header of Convenant Civiel-Militaire Bestuursafspraken (CMBA, 2005), Intensivering Civiel-Militaire Samenwerking (ICMS, since 2006) and Versterking Civiel-Militaire Samenwerking (VCMS, since 2013).

[34] This is even true for some recent cases of extreme security challenges. Terrorism has prompted many European countries to allow their police forces to walk armed through the streets. None of them would consider using 'precision-guided munition' from air- or sea-based platforms to be lobbed at their own territory. As another example, in the Northern Ireland conflict, the British Army restrained from employing heavy artillery and other massive firepower, even if that meant accepting more 'own' casualties.

[35] Note that, next to what is argued here, there is still a sound logic for having massive firepower to preserve escalation dominance and deter (peer) competitors to enter the higher ranges of the conflict spectrum.

Netherlands, to which the Constitution is subordinate, states that the maintenance of the independence and the defence of the Kingdom is an affair of the Kingdom. The Constitution holds the Dutch government responsible for the protection of the Kingdom (Article 97). Of subsequent importance are the collective defence clauses of the NATO Treaty (Article 5) and of the Treaty of the EU (Article 42.7 TFEU). These articles contain obligations to assist allies in the event of a violation of their territorial integrity. The government can only fulfil these obligations if it has freedom of action. "This is particularly crucial if there is a direct threat to Dutch sovereignty, the security of Dutch nationals or ships sailing under the Dutch flag, or the deployment security of military units, if there are no international obligations for assistance or, in the case that there are such obligations, if the Netherlands is the first responder in anticipation of international assistance (that may be limited or may not be available for some time)."[36] With (hybrid) threats that affect our vital interests directly, the chance that our Armed Forces (and other national security providers) need to act as first responder has increased.

'Agile force' profile remains valid. In the HCSS Strategic Monitor 2016 we argued that in these dynamic times: "The strategic choice 'agile force' remains the most persuasive option. The main idea behind the agile force concept is that defence organisations want to have a balanced portfolio."[37] Given the obligations stated above, this remains as true as it was in 2016 *and* in 2010, when the 'agile force'-profile (*veelzijdig inzetbare krijgsmacht*) was coined in the 2010 Future Policy Survey. The HCSS Strategic Monitor continues: "However, better mainstreaming the agility imperative that leaps out of all of our monitors is necessary." This is also very much true: higher levels of readiness, deployability and adaptability are required for quicker reaction, but also because activities such as strategic information gathering and analysis, active deterrence, probing the alertness and the will of potential opponents (probing) and creating favourable conditions for escalation (shaping, including forward deployment) take on a continuous character.[38]

The Alliance renewed. The quintessential goal under the Remain Safe Challenge is collective defence of Dutch and NATO territory. NATO is, and must remain for the period up to 2030-35, the key instrument to the government's fulfilment of its constitutional duty to guarantee Dutch territorial integrity and sovereignty. Article 5 of the North Atlantic Treaty, which enshrines solidarity between NATO member states, is essential in deterring potential enemies. However, even when NATO remains vital - by no means a given - European immense dependency on US military capabilities must change. As Foreign Affairs stated "The rift between the United

[36] Ministry of Economic Affairs and Ministry of Defence, *Memo Defence Industry Strategy*, 2018, p36.
[37] HCSS, *HCSS Strategic Monitor 2016. The Wheel of Fortune*, 2016, p28.
[38] HCSS, *Ruimte voor Vernieuwing. Capaciteitenontwikkeling van de 5e Generatie Luchtmacht*, 2019.

States and Europe did not begin with Trump, nor will it end with him. [...] The main threat to the transatlantic relationship is not a hostile White House or a decoupling of interests. Today's crisis is first and foremost a result of the power asymmetry between the United States and Europe."[39] Europe *must* take greater responsibility for, and invest more in, its own security: "Without a common vision for defence, and with destabilizing pressures on its periphery, the continent will soon serve as a theatre, rather than a participant, in a great-power competition."[40] As a middle-sized country in terms of influence in the international arena, the Netherlands is ideally suited to support strengthening Europe's military autonomy. One path is striving for a high level of force integration in Europe ('towards a European army'). This is a largely political path that has certainly utility - e.g. in promoting more interoperability in technical, doctrinal, conceptual and political sense; and in pooling or sharing strategic assets, such as strategic lift, higher level Command Posts and strategic communication networks - but little operational value (and little realism when looking 10-15 years into the future). The operational impetus for Europe's strategic autonomy our country may deliver in the period up to 2030-35 comes from cooperation arrangements with a small group of likewise nations: Germany[41]; Belgium and Luxembourg; the Scandinavian countries; France and the UK[42].

NATO's forward presence in the Baltic Region. NATO's Enhanced Forward Presence (EFP) is a forward deployed defence and deterrence military posture in the three Baltic States and Poland. The objectives of the EFP are deterrence, defence and reassurance. The EFP, however, has insufficient strength to provide a credible defence against any serious military attack from Russia, thereby undercutting not just the 'defence' but all three objectives. The EFP serves as a tripwire in order to involve other NATO members directly in case of a Russian attack. But NATO's rapid reinforcement strategy to augment the EFP has serious flaws. First, NATO's very rapid deployment capacity is very limited. In addition, it is doubtful whether the rapid reinforcement of troops is logistically possible. The EU-NATO military mobility project should eliminate bureaucratic and practical obstacles as much as possible, but even than the question remains whether the infrastructure can withstand and support massive movement of troops. Furthermore, Russia has set up a bastion defence (A2/AD) in Kaliningrad that can make reinforcement extremely expensive; and might slow Western force relocation through hybrid warfare, including sabotage and the organisation of resistance among the population. The net result is that Russian units can reach the

[39] Alina Polyakova and Benjamin Haddad, *Europe Alone. What Comes After the Transatlantic Alliance*, Foreign Affairs July/August 2019.

[40] Ibid.

[41] Modernizing the German Armed Forces in operational, strategic and political terms is of tremendous importance for a more robust European defence posture. Everything our country can do to that end through bilateral military cooperation has therefore high strategic significance.

[42] Keeping the UK fully engaged in European security is another challenge in which our country, with strong ties with the UK as well as with continental powers (particularly Germany), has a valuable role to play.

outskirts of Tallinn or Riga within an estimated 60 hours without NATO being able to do anything about it.

A credible defence of the region must therefore be carried out with in place forces. RAND calculated that in theory seven brigades, including three heavy armoured brigades supported by air power and ground-based firepower, are needed to defend the Baltic States.[43] Should this line of thought be put to practice – currently a big 'if' - it is likely that NATO will ask the Netherlands to substantially boost its current presence in Lithuania as part of the EFP.[44]

3.4 Whole of Government and Whole of Society Approaches

Great power competition and 'ecosystem' approaches

Armed Forces prepare for conflict against potential enemies. But in this era of great power competition, what is the military's (additional) role in competing with rivals? And how is the transition from competition to conflict and from rivals to enemies envisaged? These are strategic questions military strategists struggle with. Russia seems to find the answer in the 'Gerasimov doctrine'. For China, economic and political objectives are closely related. For the West, a central element is a multi- and cross-agency approach to the problem, calling for, as the US National Defense Strategy puts it, "the seamless integration of multiple elements of national power — diplomacy, information, economics, finance, intelligence, law enforcement, and military." Operationalising this 'ecosystem' approach, and the role, tasks and responsibilities of the military in it, is a key issue for the Armed Forces.

Hybrid threats require a coordinated response. Increasingly, conflicts have an impact on society as a whole. In an era where violent security threats are no longer only issued by and aimed at states and state institutions, societal resilience is of increasing importance. But whole of government (WoG) / whole of society (WoS) coordination is not easy to organise in the typically siloed governmental structures and without government control over societal stakeholders. The Netherlands organises its emerging WoG/WoS approach to security in line with its political culture: from the bottom-up rather than top-down. This does, however, provide insufficient follow-through power in the face of more severe and acute hybrid threats. We expect - and

[43] David A. Shlapak and Michael W. Johnson, *Reinforcing deterrence on NATO's Eastern Flank, RAND Corporation 2016.* https://www.rand.org/content/dam/rand/pubs/research_reports/RR1200/RR1253/RAND_RR1253.pdf

[44] HCSS will shortly publish a note, working title *Hybride Dreigingen en Hybride Oorlog: Consequenties voor de Koninklijke Landmacht*, in which this issue will be discussed in-depth.

would in general applaud - the (presumably relatively quiet) establishment of more central processes and structure mechanisms to enforce synchronisation across various government agencies and establish strategic priorities over the next couple of years. In this process, MoD must expand its role in building and supporting societal resilience against hybrid threats, such as against disinformation (see next point), both in the Netherlands and in potential conflict regions in the periphery of Europe. In other words, Defence should not just be a follower but also a shaper in the political debate and formulation of a national counter hybrid strategy. Is MoD willing and able to take on that role?

Diverging civil and military terminology for (roughly) the same threats. Lacking a top-down structure, in the current set-up in the Netherlands, the ministry of Justice and Security is the 'coordinating' ministry for national security issues. However, the terminology used by Justice and Security for societal threats induced by state actors[45] is quite different from the sort of concept common in the international military community. This confuses the required dialogue and coordination in the required WoG and WoS response to these threats.

Societal resilience to foreign interference. The role Russia played in the 2016 Presidential election in the U.S. and the Russian attempts to influence the outcome among Dutch voters in the 2019 European Parliament elections are two recent examples of 'undesirable foreign interference'.[46] Russia has a bad track record in this field. Investigating the intentions and capabilities of state actors like Russia - whether or not operating through non-state 'proxies' - is necessary to anticipate and respond appropriately to this kind of threat. Strategic communications to actively counter disinformation efforts are another critical element. MoD has a clear role to play in the former (i.e. through the MIVD), and up to a point also in the latter.[47] A more general supporting role for the defence organisation would be to raise awareness and promote individual and collective response within government organisations, vital sectors and society at large, through information, training and exercises.

Military service revisited? Citing the deterioration of its security environment, rapid changes occurring in the Baltic region, and severe deficiencies in personnel numbers, Sweden reactivated military conscription in 2017.[48] Similarly to the Netherlands, conscription was never truly abolished in Sweden, but only suspended due to

[45] See ministry of Justice and Security, Letter to Parliament *Tegengaan Statelijke Dreigingen*, 18 April 2019.

[46] "Undesirable foreign interference refers to intentional, often systematic and, in many cases, covert activities by state actors (or actors who can be linked to state actors) in the Netherlands or aimed at Dutch interests. Such activities may undermine the Netherlands' political and social system and our efforts." 2018 IISS, p34.

[47] Case in point: the press conference by the minister of Defence and the Director of the MIVD on October 4, 2018 on the Russian cyber operation at the OPCW in The Hague: https://www.defensie.nl/actueel/nieuws/2018/10/04/mivd-verstoort-russische-cyberoperatie-bij-de-organisatie-voor-het-verbod-op-chemische-wapens.

[48] Ministry of Defence, "Sweden Re-Activates Conscription," Government Offices of Sweden, March 2, 2017, https://www.government.se/articles/2017/03/re-activation-of-enrolment-and-the-conscription/.

peacetime conditions. From July 2017, conscription was reinstated and a pool of 13,000 Swedes born in 1999 were invited to apply for service.[49] With the motivation and interest of each potential recruit considered, 4,000 were selected to serve for nine to twelve months and undergo military training.[50] This number is a small fraction of the population reaching conscription age per year (over 90,000), meaning that a degree of honour and distinction is ascribed to those who are successful in joining the ranks. In turn, military service is looked upon favourably by future employers and peers. The objective is for these recruits to either remain engaged in the force professionally, or to serve in the reserves. The Swedish Ministry of Defence plans to expand conscription to more new recruits over the next six years (Figure 4).[51]

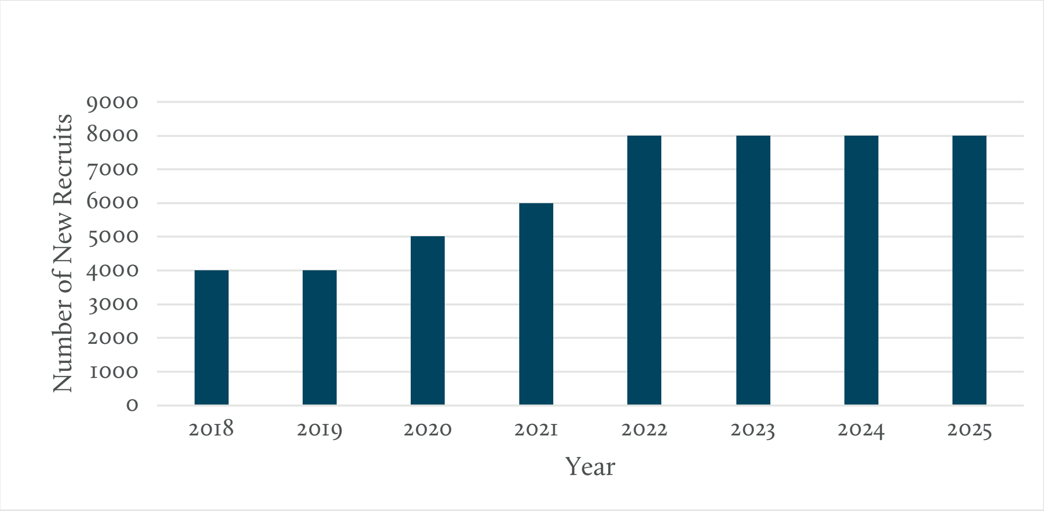


Figure 4: Projected recruitment plans for conscription in Sweden

The Netherlands could consider a similar model of hybrid recruitment, based on both voluntary and compulsory service for men and women of age. Naturally, personal motivation of each potential recruit should be considered and alternative service options made available. However, developing a selective recruitment process whereby successful applicants are highly regarded could be a necessary step to enhance the mass of the Dutch defence force.

[49] Katya Adler, “Sweden Brings Back Military Conscription,” *BBC News*, March 2, 2017, sec. Europe, https://www.bbc.com/news/world-europe-39140100.

[50] Ministry of Defence, “Sweden Re-Activates Conscription.”

[51] Ministry of Defence, “The 2015 Commission Inquiry on The Manning System of the Military Workforces Presents the Official Report,” Text, Government Offices of Sweden, September 28, 2016, https://www.government.se/press-releases/2016/09/the-2015-commission-inquiry-on-the-manning-system-of-the-military-workforces-presents-the-official-report/.”URL”:”https://www.government.se/press-releases/2016/09/the-2015-commission-inquiry-on-the-manning-system-of-the-military-workforces-presents-the-official-report/”,”language”:”en”,”author”:[{“family”:”Ministry of Defence”,”given”:””}],”issued”:{“date-parts”:[[“2016”,9,28]]},”accessed”:{“date-parts”:[[“2019”,10,4]]}}}],”schema”:”https://github.com/citation-style-language/schema/raw/master/csl-citation.json”}

4. Dynamics in To Foster Security

In this Chapter we describe some of the more salient, but possibly currently underexposed, developments that drive innovation in the Foster Security Challenge for the period up to 2030-35.

4.1 Keeping Instability at Bay

Instability in Europe's periphery affects our national security. As stated in the 2018 IISS, "(e)specially in the countries around and on the edges of Europe, the security situation has taken a radical turn for the worse in recent years."[52] The Dutch MoD is acutely aware that in our globalised world, the current security environment within the Netherlands is highly dependent on the peace and stability (or lack thereof) of not only the European periphery, but also of a wider threat landscape that transcends both national borders and the physical domain itself.[53] In this globalised world, the spill-over effects of violence resonate between communities, countries and continents. Conflict abroad affects our domestic security (compare §3.1). Social security is affected as the hosting of refugees puts pressure on communities in the Netherlands and across Europe, requiring social adjustments. Returning foreign fighters (with varying degrees of ideological extremism) could lead to an increase in ideological polarisation or to terror attacks on Dutch soil. Physical security is also at stake, as exemplified by the murder of two Dutch nationals (the first in 2015 in Almere and the second in 2017 in The Hague), allegedly directed by Iran.[54] The conflict in Ukraine produced ramifications for energy supplies to Europe from Russia, showing that our economic security is also impacted. Conflict abroad affects our state security too, in that the current tensions with Russia has led to intelligence-related activities on our territory, such as the attempted hack at the OPCW.

Security/defence priorities driven by necessity. The fact that instability elsewhere has come to directly affect security at home shapes policy. For the period to come and much more than in the past two decades, the MoD will primarily be motivated by necessity ('need to have') rather than by ambition ('nice to have'). This means that the

[52] 2018 IISS, p9.
[53] 2018 IISS, p14/p16.
[54] Daniel Boffey, "Iran behind Two Assassinations in Netherlands – Minister," *The Guardian*, January 8, 2019, sec. World news, https://www.theguardian.com/world/2019/jan/08/iran-behind-two-assassinations-in-netherlands-minister.

Netherlands is limited in the degree to which it will engage in conflict that does not directly pertain to security at home. Thus, the stated aim to "Foster Security around Europe (the Middle East, North Africa and parts of sub-Saharan Africa and West Africa)"[55] represents both a recognition that domestic security is intrinsically linked to hostile environments in Europe's 'near abroad', and an acceptance that contributions to international order and stability are explicitly selected to have a positive impact on the security of Dutch society, citizens and interests.

Small units with junior leaders doing combat, officers enabling. A crucial and far-reaching element in changing doctrines is the following. Analysis of recent and ongoing operations show that most missions today happen at the squad level, involving 14 soldiers or fewer. Decisions whether and how to apply force, both in warfighting and in stability or peace support operations, are usually made by lieutenants, sergeants and corporals, who have quietly become the military's most important battlefield leaders. Remarkably, officers have for a large part been displaced from tactical leadership. This trend isn't necessarily bad. Whereas officers typically have a broader range of knowledge and skills that allow them to evaluate the big picture; NCOs (corporals and sergeants) tend to have more combat experience and are better equipped for practical, detailed execution.

This is a developing trend for the next 10-15 years that merits attention. Even in warfighting scenarios where battalions and brigades enter combat, smaller units will likely retain battlefield authority. This is due to the devastating power and pinpoint accuracy delivered by modern artillery and airstrikes. In the combat zones of eastern Ukraine today, for instance, the Ukrainian army's movements are typically carried out by units composed of just a few soldiers. Anything larger invites crushing artillery strikes. The Dutch Armed Forces need to exploit, rather than resist, this trend. Higher rank officers will have to give up their role as tactical commanders and embrace their role as combat enablers and policy advisors. During operations, they should focus on providing institutional leadership. Higher rank officers "should think of themselves as supervisory managers responsible for coordinating between units and command and ensuring supply flows. They should also redouble their commitment to serving policy makers. Their advice should be rooted in their military experience and expertise — but not be limited to it. Civilian officials making decisions about war and peace need information filtered through conceptual lenses such as strategic theory, international relations, and other disciplines. A pure tactician can never offer policymakers the level of insight and wisdom that they require."[56]

[55] White paper, p10.

[56] B.A. Friedman, The End of the Fighting General. America's top brass should abandon dreams of battlefield glory- and focus on paperwork instead, Foreign Policy Fall 2018 issue.

4.2 Managing Security vs. Fostering Security

Securitisation of development cooperation and militarisation of border control. Not long ago, Europe sent development workers to the Sahel to dig wells. Today, European armies and security guards have entered the Sahara to block migration routes.[57] Niger is a case in point. The insignificant airport of Niamey, the capital of Niger, has in the last three years been provided with biometric equipment that links the airport computers with the security services in Europe and the US. The Americans are building a drone base worth $100 million in Niger. The French army flies daily with at least five drones over Niger and neighbouring countries to assist the more than 3,000 soldiers stationed there. French police officers also train their Nigerian colleagues to arrest migrants and their smugglers. Another example is 'blue' border control in the Mediterranean. The budget of the pan-European Frontex has exploded from €6 million in 2006 to €320 in 2018. In 2018, Frontex has started drone surveillance over the Mediterranean, in collaboration with the European Maritime Safety Agency. The investment in drones comes in parallel with the withdrawal of EU naval missions in the Mediterranean and the dissuasion of private rescue operations. But drones can only observe; boats that can save people are being replaced by drones that cannot. Furthermore, in the above processes, security is being outsourced to a booming private security/military industry with multi-billion-dollar revenues — a trend matched by the surging market for remote-controlled weapons and surveillance systems. Instability has become a business model, with parties that have vested interests in *not* providing solutions.

In short, while on the one hand we acknowledge that remote zones of insecurity may directly affect national security, on the other hand Western states, and international organisations funded and supported by them, have come to organise military, border and aid interventions in insecure zones in a dangerously myopic fashion. Through diverse forms of remote control and containment — from drones to militia middlemen, from border reinforcement to refocussed and outsourced aid — we are in effect collaborating in the remapping of the world into disjunct zones of safety and of danger, with little in between. This is a failure of imagination, opportunity and responsibility whose consequences are already coming back to haunt us.

Migration as a security issue. In extension, migration is increasingly presented as a security issue, rather than a human rights issue. Migration is now mentioned in the same breath with societal unrest and terrorist attacks. Refugees are portrayed as a religious and financial danger that requires security (including military) measures. This is a dangerous trend. Military forces can, up to a point, provide basic security as a prerequisite for the development of fragile states. The development process

[57] https://www.nrc.nl/nieuws/2019/08/06/drones-in-plaats-van-waterputten-voor-afrika-a3969281

itself requires quite different expertises, capabilities and mindsets than Armed Forces possess. As the Swedish anthropologist Ruben Andersson points out in his recent book *No Go World*,[58] militarisation of borders does not solve the problems of migration. “It actually increases the stress on the borders, the chaos, and the number of fatalities,” he says. “Compare this with the response to 9/11. After the very expensive War on Terror, the number of victims of terrorist attacks worldwide has increased tenfold, from 3,000 victims in 2000 to 29,000 victims in 2016. Action made the problem worse.”

How to ‘foster’ security; role of the military. A basic principle in international relations is that sovereign countries are responsible for their (own) national security. The problem of many countries in Europe’s periphery is that they are insufficiently able to provide for their own national security. The result is a spill-over of all kinds of problems from one sector to another and from one country to others. For the EU and its member states this results in a policy dilemma (or rather a question of balance): focus on the ‘securitised’ consequences / symptoms and try to control or at least contain these; or accept the basic premise that in many countries the security sector is too weak and needs outside help, for example in the form of capacity building and support. Within the context of the current national and institutional agenda in the Netherlands and in Europe, the focus today is on the former; with the sustainable latter response receiving less - in our opinion: not enough - attention.

Although the military are primarily associated with the security side of things (and are indeed deployed in that sense, even in civilian missions such as Frontex), having beared witness to the dynamics present in fragile states and danger zones, they know, possibly better than anyone, the limitations of military solutions. They have experienced how ‘military responses designed through a myopic security lens (and, increasingly, through vested multi-billion business interests) could actually make things worse; and certainly don’t provide for sustainable solutions. What the military *can* do is twofold. Firstly, they can help in creating the level of stability and security that is required for being able to implement more long-term capacity and state building. Secondly, they can provide a small but important part of this through assistance in Security Sector Development (SSD). In the debate on how to tackle instability at Europe’s (southern) borders and, for instance, the migration flows associated with it, based on their professional experience the military should be more outspoken and more being heard in order to add a healthy sense of realism to the debate.

[58] Ruben Andersson, No Go World. How Fear Is Redrawing Our Maps and Infecting Our Politics, April 2019.

4.3 Persistent Local Presence

The 'included' added value of 'inclusive' Foster Security missions. As Table 3 shows, most current military missions are associated with the Foster Security Challenge.[59] Detached from their primary objectives (as e.g. discussed in §4.2), all these missions have, in varying quantity and quality, generic added value. They provide the opportunity for obtaining on the ground information regarding the local security situation. Local relationships are being created or fostered. Even limited local presence can be crucial as a stepping-stone for more substantive missions or as a source of intelligence for security risks that may affect Dutch interests. However, continuity is a prerequisite; if not, local contacts and local knowledge crumble. A longer-term approach towards a few focus countries, with combined diplomatic, military and development efforts, is crucial. Furthermore, as the world tends to move downwards in the Framework in Chapter 2, the role of state actors is increasingly augmented by non-state actors performing relevant functions for maintaining and restoring stability in vulnerable regions. Current examples include Alphabet and Amazon which, in a mix of corporate social responsibility and business opportunity creation, bring free internet to large parts of Africa; the education, healthcare and gender equality development projects undertaken by the Melissa & Bill Gates Foundation; and the economic governance, equality and antidiscrimination projects sponsored by the Open Society Foundations of George Soros.

Accordingly, it has never been truer that threats that pertain to the Strategic Challenge Foster Security will typically play out in a collaborative setting with multiple stakeholders and the international community forming coalitions and joint mandates in order to engage 'as a whole'.

[59] There is, of course, a bias associated with the word 'mission'. The substantial Dutch presence in the Caribbean part of the Kingdom is not labelled as a mission. Activities in the intelligence sphere or in the cyber domain are no missions. Neither are naval ship itineraries, large training exercises abroad. The substantial burden of national tasks, such as the tasks of the Royal Marechaussee, coast guard duties, national air space protection and ordnance disposal, is also disregarded in this table.

Mission	Deployed personnel (2018)			International framework	Location	Challenge
	military	civil	total			
Europe						
eFP	657	0	657	NATO	Lithuania	Remain Safe
EULEX Kosovo	2	15	17	EU	Kosovo	Foster Security
Middle East						
Combating ISIS						
ATFME	652	0	652	Coalition	Jordan	Foster Security
PED - TSC	59	0	59	Coalition	Netherlands	Foster Security
CBMI	369	0	369	Coalition	Iraq	Foster Security
A&A	45	0	45	Coalition	Iraq	Foster Security
Chirurgical team	40	0	40	Coalition	Iraq	Foster Security
NMI	2	2	4	NATO	Iraq	Foster Security
UNIFIL	1	0	1	UN	Lebanon	Foster Security
UNDOF	6	0	6	UN	Israel	Foster Security
UNTSO	24	0	24	UN	Israel	Foster Security
EUBAM Rafah	0	0	0	EU	Israel/Palestinian Territories	Foster Security
USSC	10	1	11	Coalition	Israel/Palestinian Territories	Foster Security
Africa						
MINUSMA	747	27	774	UN	Mali	Foster Security
EUTM Mali	2	0	2	EU	Mali	Foster Security
EUCAP Sahel Mali	0	3	3	EU	Mali	Foster Security
EUCAP Sahel Niger	0	2	2	EU	Niger	Foster Security
EUBAM Libya	2	1	3	EU	Libya	Foster Security
EULPC Libya	2	0	2	EU	Tunisia	Foster Security
EUNAVFORMED Sophia	2	0	2	EU	Rome, Italy	Remain Safe
Operation Sea Guardian	300	0	300	NATO	Mediterranean	Foster Security/ Secure Connections
EUNAVFOR ATALANTA	6	1	7	EU	Northwood, UK	Foster Security/ Secure Connections
EUTM Somalia	6	0	6	EU	Somalia	Foster Security
UNMISS	12	0	12	UN	South Sudan	Foster Security
ACOTA	24	0	24	Coalition	Burkina Faso, Uganda	Foster Security
Central Asia (Afghanistan)						
Resolute Support Mission	450	0	450	NATO	Afghanistan	Foster Security
CMF	6	0	6			Secure Connections
National						
VPD	220	0	220			Secure Connections
	3646	**52**	**3698**			

Table 3: Dutch military missions in 2018[60]

[60] Source: bureau Evaluaties, Defence Staff. Individual postings are not mentioned.

4.4 Cities as Key Military Terrain

The urban dilemma. In the next 10-15 years, security issues are likely to play out in an urban(ised) environment. The world is increasingly characterised by a patchwork of large urban agglomerations that not only constitute economic centres of power, but also compete for political power. Large cities have a pivotal economic, social, cultural and political function, but are also vulnerable to security problems. They are, for example, places of refuge for organised criminal networks and breeding grounds for terrorism. Global interests, and therefore conflicts of interest, will be more and more connected to and focused on urban centres. Instruments of power and influence - including military power - will increasingly be applied in urban environments. Armed Forces face a dilemma: preferably they stay away from urbanisations to avoid casualties, collateral damage and, in general, a complex landscape of ground, above ground and underground infrastructure that is difficult to oversee and impossible to control.

Operating in cities places specific demands on personnel, platforms, (unmanned) systems and command and control.[61] High-tech long-range weapon systems and large platforms have limited use, while the utility of soldiers (boots on the ground) and small systems increases. And certainly, in Foster Security missions, military actions must blend in with a much wider range of other activities, an integrated approach. 'Smart' technology combined with more agile TTPs[62] is required. This technology is essentially civil-based and partly already present in the extensive infrastructure urban environments offer and that can be utilised to render military operations more effective and efficient. Some technological elements for urban operations are small or miniature sized airborne unmanned systems as well as hunter-killer UAVs to counter the drones of opponents; relative small and versatile, increasingly electric and autonomous vehicles capable of delivering equipment, ammunition or personnel; lightweight personnel protection; and hand-carried systems that use available infrastructure (all kind of sensors in the public space; public communication networks etc.) to maintain situation awareness and to communicate.

[61] One of the "seven spearheads for the renewal of the Armed Forces" in the *Strategische Kennis en Innovatieagenda 2016-2020. Vóórblijven in een onveiliger wereld* of the Ministry of Defence is (better) urban operations. The recent Army vision, *Veiligheid is Vooruitzien. De toekomstvisie van de Koninklijke Landmacht*, also stresses the need for improving the ability to operate in build-up areas.

[62] Typically, urban military operations require military units to have well trained-in Tactics, Techniques and Procedures (TTPs). However, opponents could use fixed TTPs against us. Flexibility is therefore key to success. One of the tactical solutions would be to use a 'playbook' (the concept taken from American Football) with 'plays' that can be used in different situations, with an element of surprise to the opponent included.

5. Dynamics in To Secure Connections

In this Chapter we describe some of the more salient, but possibly currently underexposed, developments that drive innovation in the Secure Connections Challenge for the period up to 2030-35.

5.1 Connections, Flows and Economic Wars

Secure Connections as a (new) key challenge.[63] Let us first consider this relatively new concept of Secure Connections, also known as Flow Security (see textbox below), that now stands on par with the more familiar challenges of territorial defence of Dutch and NATO territory (Remain Safe) and of promoting global stability and maintaining the international order (Foster Security). This notion acknowledges two things. First, that in the age of globalisation, world-wide connections and the flows these connections facilitate yield enormous economic, social, and cultural value, whether through trade, foreign investments, tourism or the exchange of knowledge and ideas. Second, that these connections and flows are vulnerable to intentional or accidental disruptions with possible cascading effects. International physical and virtual connections run through the global commons (the high seas, space, cyber space) with often no clear demarcation as to who exactly is responsible for the security of the connecting medium and the flows themselves. This is certainly the case for information; and communication networks are typically borderless. And while most of the hubs in the global flow networks are physically located on the territory of a state, this does not necessarily mean that the state is fully responsible for the security of the hub because much of the infrastructure is in the hands of private companies. Criminal and terrorist organisations consequently exploit these security flaws and holes in the flow infrastructure. And states worldwide, including Russia, China and Iran, have been beefing up their Area Access and Aerial Denial (A2/AD) capabilities, allowing them – next to defending their own assets – to credibly threaten others with denial of access to Sea, Air and Land Lines of Communication.[64]

[63] As the *Wetenschappelijke Raad voor het Regeringsbeleid* (WRR) noted in its 2017 appreciation of Dutch defence strategy, "Economic security and Flow Security have only quite recently been put explicitly on the Dutch security agenda and are not embedded as full-fledged perspectives in the broader policy".

[64] HCSS, Flow Security and Dutch Defence and Security Policies, 26 February 2018 https://www.hcss.nl/sites/default/files/files/reports/Flow%20Security%2012012018.pdf

Secure Connections and/or Flow Security

These terms essentially denote the same, but with a different emphasis. Secure Connections highlights the infrastructural component, the lines of communication or LOCs, whereas Flow Security stresses the content, the physical goods or virtual communication messages themselves. The two are intrinsically linked: flows cannot exist without a connection medium; a connection that is void of content is useless. Here, we use the two terms interchangeably, but with the distinction in accent as indicated. In the virtual domain, there is a similar distinction to be made between the cyber domain (or 'cyberspace') and the information domain. The former primarily refers to the ICT infrastructure (hardware and software) for storing, processing and sharing information; the latter to the (digital) information that resides on this infrastructure, its meaning as well as its *perceived* meaning when used in human interaction (think of media manipulation). In day-to-day parlance, however, cyber domain and information domain tend to indicate more or less the same. In practical military terms, cyber operations (aimed at information *infrastructure*), information operations (aimed at the *content* of data / information / intelligence) and psychological operations (aimed at the human *understanding* of information) are often closely associated and/or overlapping. Again, we here use the two terms interchangeably, but with the distinction in accent as indicated.

Worldwide flows and Dutch prosperity. A major part of Dutch prosperity and well-being depends on the worldwide physical and digital connections of our country. The reverse also holds: the global economy has a significant dependence on our country's hubs, to transit commodities (Port of Rotterdam), people (Schiphol Airport) and data (Amsterdam Internet Exchange, various huge data centres and server farms) between the world's landmasses. This earns the Netherlands a unique position as a 'systems country' within the global economy - a function which has earned it its appellation 'the gateway to Europe', and which is reflected in its top-5 positions on globalisation-related indices such as the WEF Enabling Trade Index, the KOF Index of Globalization, the DHL Global Connectedness Index and the McKinsey Connectedness index.

Contemporary wars are essentially economic. Both massive and precision fire power are now universally available for both state and non-state actors. Threats to use massive firepower may be rendered ineffective by counter-threats to do the same. The situation in Yemen provides good examples: the threat of bombing Dubai forced the Emirates to seek Iranian mediation. The Houthis, despite years of Saudi bombing of Yemen, have also managed to bomb airports, military bases and oil stations in the heart of Saudi Arabia, using cruise missiles and armed drones. As a result, geopolitical and regional conflicts tend to manifest themselves differently. We see wars of sanctions; we see obstructions to the free movement of ship movements around the globe. We currently witness a war of tankers and oil platforms in the Gulf and Strait of Hormuz. These are starvation wars, in which global connections (and the ability to disrupt them) play a prominent role. In such confrontations both 'soft' and 'hard' instruments of national influence may be brought to bear. Traditional divisions in terms of responsibilities and tasks are shifting in this dynamic landscape (see example in text box).

Role of Defence in on-board protection against piracy

The Dutch MoD makes Marines available for so-called Vessel Protection Detachments (VPD) on board of ships crossing piracy-prone international waters. In 2018, the House of Representatives decided to allow armed private security guards on merchant ships, so ship owners can hire security guards if military protection is not available. This issue has been on the Dutch political agenda for years. There was not enough support for earlier proposals, when the majority of the Representatives did not want to deviate from the State's monopoly on violence.

The above exemplifies a more abstract debate on the role of the defence organisation (i.e. the state) in relation to other - public, public-private or private - security providers. In this debate, on the one hand, expansion of the role of the military in traditionally non-military arenas - such as building resilience as part of conflict prevention - is discussed, while on the other hand the monopoly of the Armed Forces / the state on the use of violence is no longer sacrosanct, as the example shows.

Globalisation reversed? Will the (new) emphasis on global connections be a continuing trend for the next 10-15 years? Not necessarily. The golden age of globalisation is over. It has given way to a new era of sluggishness, what the Economist calls "slowbalisation".[65] The cost of moving goods has stopped falling. Multinational firms have found that it is increasingly difficult to compete with local rivals. Activity is shifting towards services, which are harder to sell across borders. Trade and tariff wars are raging. The dominant neo-liberal view of how the world system best functions (i.e. with as little obstacles for free trade, technology transfer etc. as possible) is being challenged by competing ideologies. One of the big systemic trends for the next

[65] https://www.economist.com/leaders/2019/01/24/the-steam-has-gone-out-of-globalisation

decade might be the economic decoupling between large economic blocs, in particular between the US and China (see text box). Decoupling would involve disentangling complex supply chains established over many years. A big unknown is how Europe features in this global game. The net result might well be a relative or even absolute decline of the use of global lines of communications. The emergence of 'borders' in the global internet (leading to what is dubbed 'splinternet'[66]), under Chinese impetus, is a case in point.

Fragmentation of the world economy

President Trump's trade policy against China is not protectionism in the sense of trying to help a domestic industry in its struggle against imports. The goal is much broader and more significant: the economic decoupling of the United States and China. That would mark a historic fragmentation of the world economy; or, in the words of former US Treasury Secretary Henry Paulson, the falling of an "economic iron curtain" between the world's two largest economies. Such a separation would have foreign policy and national security implications well beyond the economic consequences. If Trump remains a one-term president, many of his policies can be reversed. But the tariffs on China are a game changer. Any future administration would have a difficult time removing them without sizable concessions from the Chinese leadership and some way of alleviating the national security fears that now dominate the bilateral relationship. And if Trump wins re-election and continues down the path of economic nationalism, the prospect of continued, and perhaps intensified, trade conflict is likely to do incalculable damage to the world economy. As Foreign Affairs puts it: "In the worst-case scenario, the new world trading system will be dominated by discriminatory trade blocs that raise the costs of commerce, make trade negotiations harder, and encourage retaliation. Size and economic power, not principles or rules, will determine the outcome of trade disputes. Such a system will hurt smaller, weaker countries and could push them to align with more powerful ones for self-preservation."[67]

5.2 Protecting Sea Territory and Sea Infrastructure

The increasing economic value of the sea. A major characteristic that previously distinguished land from maritime territories was the presence of population and economic assets that needed to be defended. That contrast is fading. Maritime areas increasingly have inherent economic value associated with trade routes,

[66] https://en.wikipedia.org/wiki/Splinternet

[67] Chad P. Bown and Douglas, A. Irwin, Trump's Assault on the Global Trading System And Why Decoupling From China Will Change Everything, Foreign Affairs September/October 2019 Issue.

natural resources (including fisheries), offshore installations and undersea cables and pipelines. In recent years, we have witnessed — and will continue to witness in the period up to 2030-35 — a proliferation of infrastructure development both above and below sea level. Communication cables make up for more than 90% of all communication traffic between the US and Europe. Seabed cables are also used to transport energy. This is particularly the case in the North Sea, from the European mainland to the UK and Norway. With the construction boom of offshore wind parks, the number of seabed electricity cables will sharply rise. Because of their location and length, 24/7 monitoring—let alone protection—of seabed cables is a challenge.

Seabed warfare. With the surge of submarine cables and pipelines, a new form of warfare is emerging, called seabed warfare. Fears of Russia's capabilities for cutting, disrupting or wiretapping undersea communication lines are growing, while a lack of formal state ownership means the cables do not have strong protection in international law. A concrete manifestation of Russia's capacity in this field is the Yantar, a special purpose intelligence collection ship said to carry "advanced surveillance equipment, including a remotely operated underwater vehicle and two manned submersibles that the BBC reported can dive to about 6,000 meters."[68] Energy cables and oil and gas pipelines are equally vulnerable, difficult to monitor continuously, and impossible to protect completely. The consequences of disturbing the throughput will be felt severely in Western Europe and in the Netherlands, where the dependence on imported gas increases as a result of the shutting down of the Groningen gas fields. However, disturbances of, say, the Nordstream 1 and 2 pipelines between Russia and Germany are not in Russia's interest. But these multi-billion investments provide Russia a good reason to ramp up defences relevant to securing the pipelines. The pipeline's underwater depth is perfectly suited for the type of surveillance equipment incorporated in Russia's plans for an underwater acoustic surveillance system as part of its A2AD capability portfolio.

In short, monitoring of and safeguarding offshore installations and undersea cables is required, but not an easy task. Persistent presence and overview, based on superior and timely intelligence capable to counter opponents and saboteurs, is needed and requires sufficient capabilities, possibly to a large extent unmanned (see text box below), to do so.

The threat of sea mines. Another military task that warrants more attention is mine clearing. Sea mines are the poor man's weapon of choice to limit access to harbours. The increasing number of wind parks in the North Sea Channel limits shipping to relatively narrow corridors, making it easier to disrupt transit. Sea mines are mass produced and worldwide available. Deployment is a simple task and can be done overtly from naval vessels or covertly from commercial ships. This makes sea mines the

[68] https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables

ultimate asymmetric weapon. One oil tanker sunk by a sea mine in the North Sea could bring traffic to Rotterdam to a stand-still, with potentially multi-billion economic losses (next to huge environmental damage). Even the threat of sea mines could cause severe disruption in the sea lines of communication. Besides this kind of 'shock' use, sea mines can be used strategically, channelling or denying passage through restricted waters and in and out of ports needed for sustenance of naval operations. They can shape the naval battlespace and the approaches to it. Used tactically, they can slow or stop movement to and through narrow straits and to landing zones on beaches, and in so doing can also make a slowed or stopped force more vulnerable. Legally, there is no restriction to laying mines in international waters, as long as it is advertised in which area these mines are deployed, in order for civilian shipping to evade these areas. In response, there is a need to develop and maintain a superior intelligence position for situational awareness of the threats posed to ports and littoral waters; and adequate sea mine detection and clearing capacity.

Unmanned maritime systems (UMS) for a wide range of naval tasks

The recent decision of Belgium and the Netherlands to jointly develop a toolbox of unmanned systems for mine-countermeasures[69] might be extremely significant beyond the direct area of application. This approach could be turned into a holistic concept for applying UMS for a wide range of maritime tasks. We already referred to UMS in the context of seabed warfare. Another example would be the application in grey zone activities as these currently unfold in the Persian Gulf, the Strait of Hormuz and the Arabian Sea.[70] The Iranian seizure of a Swedish oil tanker under British flag was a culmination point of ongoing activities, such as harassing commercial vessels with speedboats. Staying out of the region for an interim period, as the British government has advised U.K. shipping, has been interpreted as a watershed moment "when the UK admits it can no longer protect its merchant vessels."[71] Enter stage: UMS. In the Arabian Sea, UMS would be ideal to counter Iranian "mosaic defence"[72] because they can be built to be lost. This levels out current asymmetries between speed boats and big capital ships. But the mission envelope of UMS could be much broader. UMS can collect intelligence and provide reconnaissance; push the defence perimeter out; be used for deception operations; and constitute the outer ring of maritime protection missions. The technology is largely there; it is innovative concept development that is required most.

[69] https://www.navalnews.com/naval-news/2019/06/opening-the-toolbox-ecas-solution-for-the-belgian-dutch-mcm-program/

[70] Example based on http://cimsec.org/why-unmanned-systems-are-the-go-to-option-for-gray-zone-ops-in-the-gulf/41187

[71] https://www.savetheroyalnavy.org/irans-illegal-seizure-of-a-british-tanker-a-failure-by-the-royal-navy-or-a-failure-of-strategy/

[72] https://iranprimer.usip.org/resource/irans-military-doctrine

War over Fish.[73] The United Nations currently estimates that Earth's population will grow from 7.6 billion mid-2017 to 9.8 billion in 2050, a 29% increase. Simultaneously, hundreds of millions of people are likely to rise to middle class level. To maintain political support at home, leaders must ensure access to the high-quality food that is part of a middle-class lifestyle - with fish an important element in that diet. But the supply cannot keep up. All around the world, seas are being overfished. Scarcity has already forced Chinese fishing fleets further and further afield in search of their catch.[74] Such harvests comprise somewhere from 20% to 50% of the global catch and inflict economic, social, and environmental damage on some of the world's most vulnerable populations as fisheries collapse from overfishing. Rural fishing communities wrestle with the subsequent loss of income and, eventually, their social fabric. The classic example is fishermen in Central America turning to drug cartels for employment or poaching from closed fisheries, feeding the cycle of violence and environmental damage.

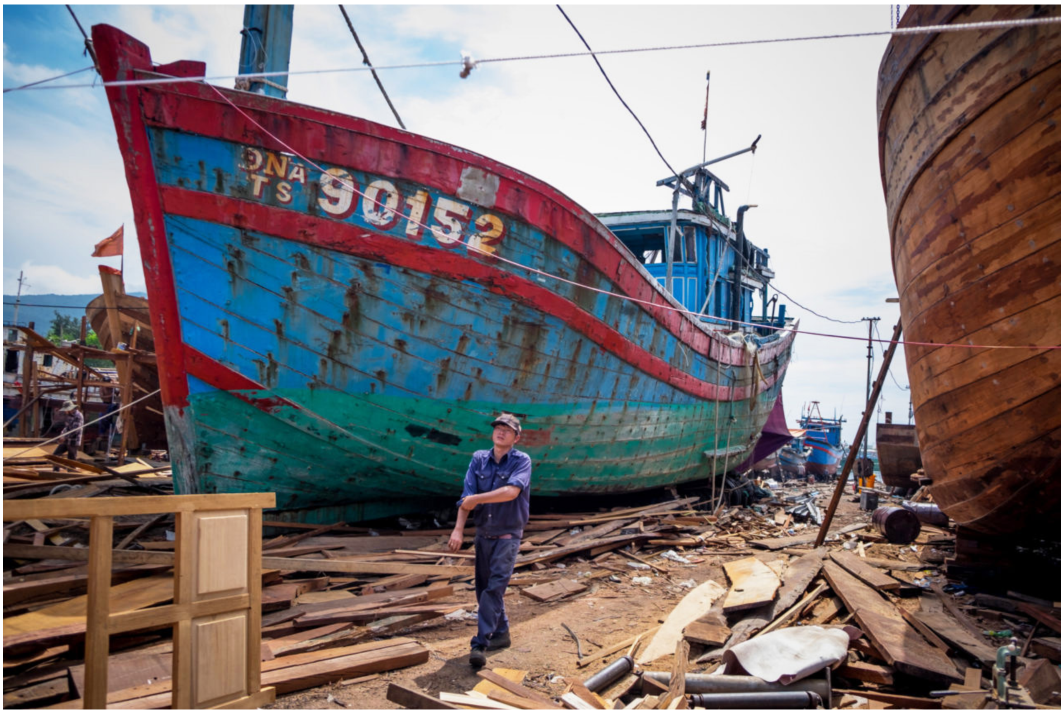


Figure 5: damaged Vietnamese fishing boat, which was reportedly rammed by a Chinese ship in the South China Sea (source: STR/AFP/Getty Images)

The political leaders of rising powers will feel enormous pressure to secure the resources their citizens demand, even if it means violating international norms and rules. This pressure sows the seeds of potential conflict in two distinct ways. The first

[73] Based on Kate Higgins-Bloom, *Food Fight. Why the next big battle may not be fought over treasure or territory but for fish*, Foreign Policy Fall 2018 Issue.

[74] China has the world's largest distant-water fishing fleet, with more than 2,500 vessels, and has been accused of industrial-scale fishing in waters as far away as off the coast of Senegal and Argentina, where China cannot even pretend to have territorial claims.

is that some states will overplay their hand when using fishing fleets and fisheries enforcement to exert influence in contested waters. The second is that illegal fishing by some nations, driven by exploding domestic demand and collapsing supply, will be met with increasingly aggressive enforcement by other nations - which could quickly escalate and spill over into actual conflict. The return of great-power competition has increased the likelihood of a war over fish.

Fish Wars in the Caribbean part of the Kingdom of the Netherlands.

Consider a hypothetical but plausible example in which Venezuelan President Nicolás Maduro trades his country's fishing rights to China, as other impoverished countries have done, to cover part of Venezuela's $60 billion in outstanding debts. China would then have legal claim to Venezuelan waters, some of which are contested given Venezuela's history of border disputes. The demarcation of Venezuela's Exclusive Economic Zone could, in theory, extend beyond the Antilles. Furthermore, the dormant claim that the Antilles belong to Venezuela could, once again (like then president Chavez did in 2005), be revived. If Beijing continues to expand the practice of escorting its fishing fleet with armed China Coast Guard vessels, in such a scenario the chances for a violent exchange with the Netherlands would be significant — as would the risk of the United States becoming involved.

5.3 Protecting Information Flows

The Dutch stake in free and borderless information flows. The future of the Netherlands is as much dependent on the free flow of value adding ideas, information and technology as it is on undisturbed physical flows. Information and financial flows accompany trade flows and make them possible. Vice versa, digital flows are facilitated by the physical domain, i.e. the servers, routers and cables of the global internet. In many aspects, the internet functions as a global common, much in the same vein as the high seas. Up to a point, international rules and norms regulate internet security issues, but in the end it comes down to the 'international community' *and* (this is where the global internet strikingly deviates from the high seas) a host of private and societal actors willing and able to enforce these rules and norms. But this in turn is at odds with a whole palette of information and financial networks that are also part of the network of networks that the internet constitutes and that are tightly controlled by private parties. Furthermore, next to positive digital flows that need to be protected, there are negative flows, such as the information and financial flows (e.g. through the dark web) that facilitate illegal arms trade and drugs and human trafficking, that require containment. Small wonder that this complex structure and intricate world wide web, full of seams between areas of interest and of responsibility, is subject to manipulation and attack.

The asymmetry of cyberattacks. Cyberwarfare by nature is asymmetric. Single persons can find and exploit small holes in the massive defences of countries and huge international corporates. In all likelihood, it won't be cutting-edge cyberattacks that may cause the much-feared cyber-Pearl Harbor in Europe or the US. Instead, it plausibly will be mundane strikes against industrial control systems, transportation networks, and health care providers — because their infrastructure is out of date, poorly maintained, ill-understood, and often unpatchable. Possibly even worse will be the invisible manipulation of public opinion and election outcomes using digital tools such as targeted advertising and deep fakes—recordings and videos that can realistically be made via artificial intelligence to sound like any world leader. The great challenge for the Armed Forces is that the rules that apply to cyberwarfare are not the ones intuitive to military versed in fighting conventional wars. As an example: in cyberspace, if an enemy wants to ground air power, he doesn't go through the front door, the fighter jets themselves. He goes after the airport, after the logistics systems and after the iPads the pilots take home.[75] There are no stand-alone entities anymore — everything is part of a network. Setting up perimeters might help, but are never watertight, while at the same time the real threats in cyberspace come from the inside.

Set in the larger security landscape, however, cyber defence is a relatively predictable component of protecting the national (and the global) ICT infrastructure. While cybersecurity experts can't have perfect certainty over attribution or even the existence of some attacks, in this broader picture the risk of cyberattacks is knowable, probabilistically. Cyber defence isn't magic. It's plumbing and wiring and pothole repair. It's dull, hard and endless.

Role of the military in cyber protection. Protecting the national ICT infrastructure against cyber intrusions and attacks in all its forms[76] is clearly a whole of government and whole of society effort. Within the Dutch government, the Ministry of Justice and Security has *coordinating* responsibility, with various other government agencies having their own field of (operational) responsibility. The role of the MoD and the range of its activities in this is not yet clearly demarcated; and might substantially grow in the years to come. Some hold that (re-)allocating considerable assets to cyber capacities dilutes the ability of the military to perform its core tasks in the physical domains. We oppose this notion. In the transition to an information society, information inevitably becomes the nexus of clashes of interest. Information is a means, but increasingly also a target and a weapon. The MoD should have prime responsibility for offensive cyber operations as well as for the defence against offensive cyber operations of state opponents. Since offensive and defensive cyber

[75] Or after the pilots' family, see https://www.nrc.nl/nieuws/2019/08/09/telefoontjes-als-vorm-van-goedkope-oorlogvoering-a3969607

[76] See e.g. https://www.government.nl/topics/cybercrime/forms-of-cybercrime

operations are closely linked - Computer network defence (CND) is insufficiently effective without computer network exploitation (CNE) and computer network attack (CNA) - offensive and defensive capabilities and actions need to be integrated. Next to strengthening cyber capabilities, the defence organisation must create a better understanding of legal constraints, on moral and ethical boundaries and on the actual planning and conduct of offensive cyber operations; and must do so embedded in a national and international 'cyber defence' ecosystem.

Cyber deterrence. With conflicts increasingly fought over, with and through information, deterrence in the cyber/information domain becomes a quintessential task of the defence organisation. Cyber deterrence, like conventional deterrence, combines (1) deterrence by denial and (2) deterrence by punishment. In a modern approach to (cyber) deterrence, these are augmented by (3) measures to create entanglements and (4) programs to set norms and standards.[77] Entanglement refers to the existence of various interdependdencies that make a successful attack simultaneously impose serious costs on the attacker as well as on the victim. If there are benefits to the status quo and its continuation, a potential adversary may not attack because it has something highly valuable to lose, and this contributes to deterrence. Normative considerations can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack. Both entanglement and norms can impose costs on a (potential) attacker even if the attack is not denied by defence and there is no retaliation. The defence organisation must strengthen its capacities for cyber deterrence in all four areas of denial, punishment, entanglement and norm setting, again in close cooperation with ecosystem partners.

5.4 Space Security

Space security / space awareness. This security aspect is not specifically mentioned in the 2018 IISS. This is an omission because space is a global common that is indispensable for major global communications and navigation networks, and one that provides crucial earth observation data for scientific and commercial purposes.[78] From space, observations can be made without violating a nation's sovereignty. But space is on the brink of becoming militarised. The US, Russia, China and India are developing offensive capabilities against satellites. The destruction of military assets in space would result in great risks for the civilian use of space, because of dual-use systems and the creation of space debris. Since this would have an effect on

[77] Joseph S. Nye, *Deterrence and Dissuasion in Cyberspace*, 2017.

[78] See e.g. the brochures https://hcss.nl/report/folder-belang-en-toepassing-van-aardobservatie; https://hcss.nl/report/folder-aardobservatie-en-veiligheid; and https://hcss.nl/report/folder-aardobservatie-voedsel-klimaat-en-biodiversiteit;

the whole world economy, it will probably limit the use of space weapons by state actors, but possibly less so by certain non-state actors. The defence organisation will have a leading role in space security and space awareness. Investments should be made in space-based and earth-based infrastructure - such as receivers, control assets, responsive space capabilities and space situational awareness projects - and in sufficient personnel. In June 2019, the updated Dutch space policy was presented to Parliament. This is the first high level government paper in which the connection between the space domain and security and defence is mentioned.[79] Furthermore, 'Security in and from space' is one of the eight missions under the Security theme of the top sector policy of the Ministry of Economic Affairs (see text box).

Security in and from space

In July 2018, the government adopted a mission-driven innovation policy. It focuses on five social themes, including the Security theme. In a consultation process of representatives of government, the business community and knowledge institutions, eight missions have been formulated, with the prospect of concrete innovations for operational users at the ministries of Defence and Justice and Security, and economic opportunities for business. One such mission is labelled 'Security in and from space', with the following aim: "In 2030, the Netherlands will have an operational deployable space capacity for Defence and Security. Space capacity includes both satellites, ground infrastructure and the possibility of information processing. With an operational space capacity we can make an essential contribution to safety by protecting the critical space infrastructure; making optimum use of satellite applications for tracking moving objects, detection of emissions, illegal behaviour on the earth's surface, changes, vegetation drought, observation and secure communication; and protecting against threats from space (objects, solar storms, spectrum disturbances, unwanted observation etc.)."[80]

[79] https://www.rijksoverheid.nl/ministeries/ministerie-van-economische-zaken-en-klimaat/nieuws/2019/06/19/kabinet-kiest-bij-investeren-in-ruimtevaart-voor-maatschappelijk-belang

[80] https://www.topsectoren.nl/innovatie/documenten/kamerstukken/2019/april/29-04-2019/missiedocument, p64.

6. Where the Strategic Challenges Meet

Although each of the three Strategic Challenges has a clearly distinct narrative, these narratives are also very much intertwined. "Security is indivisible" may be a politically convenient phrase to smooth over international or institutional dividing lines, but it is indeed based on a real interconnectedness that is a reflection of our age. In this Chapter, we highlight some essential, but possibly underexposed, elements of this overlap and continuity between the Strategic Challenges.

6.1 A Holistic Approach to Security

Development and security. Over 16,000 personnel from 39 NATO member states and partner countries are currently deployed in support of NATO's Resolute Support Mission in Afghanistan. So, what is NATO doing in Afghanistan, quite distant from the NATO territory; what is the 'collective defence' issue here? This can be seen as a complex question requiring a lengthy answer that will certainly reference the events in New York and Washington of September 11, 2001 to explain NATO's presence in Afghanistan almost 20 years later. A simpler answer is that the Remain Safe and Foster Security Challenges are closely linked and mutually reinforce each other in achieving the desired effects. The two Challenges go hand in glove in being proactive and responsive in crises, wars and instability, thereby trying to prevent, or at least control, large(r) flows of refugees and migrants; the spread of terrorism and international crime; and spill-over (from a region to adjacent regions) and cross-over (from one sector to another) effects from local or regional instability. As the 2018 IISS notes: "[c] onflict prevention is [...] important for both development and security."

Promoting the international legal order (in cyberspace). Trade heavily depends on trust between partners. A rule-based global order facilitates and installs trust. Security and the legal order are closely interlinked. Promoting the legal order in itself is not a military task. But creating the conditions for making that goal possible might be, in particular in (physical and virtual) regions prone to instability and insecurity. This is where the Foster Security and Secure Connections Challenges meet. A particular example in which the Netherlands has an ambitious role is in "promoting stability in cyberspace to build peace and prosperity". This is the motto of the Global Commission on the Stability of Cyberspace (GCSC), sponsored by the Dutch Ministry of Foreign Affairs. The GCSC develops proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behaviour in cyberspace, such as through the November 2018 *Norms Package Singapore*.[81] In the elaboration and enforcement of such norms and standards, although primarily a civil task, the defence organisation has a distinct role. An example would be in the detection, prevention (e.g. through deterrence) and response of offensive cyber operations by non-state actors, in the extension of norm 7 of the Norms Package Singapore: “Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur.”

Critical Infrastructure Protection (CIP). Within CIP, the Secure Connections and Remain Safe Challenges meet and overlap. The vital infrastructure in the Netherlands is divided into nine vital sectors: energy, ICT/Telecom, drinking water and water, transport, the chemical industry, the nuclear sector, the financial sector, digital government and Defence. CIP as a whole is generally seen as part of the Remain Safe Challenge. However, for the sectors energy, ICT/Telecom and financial, international flows and networks are central. We therefore consider the integrity of international energy, ICT and financial networks part of the Secure Connections Challenge.

6.2 Three Challenges, one Armed Forces

Multi-domain, multi-level operations. The Netherlands does not have the budget nor, given the integrated nature of many security issues, the requirement for separate, Challenge-specific forces. In fact, if anything, we are moving towards further integration of the various branches of the Armed Forces (see text box below). Technological developments are fundamentally changing the character of warfare. Decision cycles are speeding up with increased automation and autonomy. With cyber and space augmenting the traditional operational domains of land, sea and air, the dimensions of manoeuvrebility at the tactical, operational and strategic levels are being expanded. Long distance precision weapons sew the physical domains together. Today, joint operations are routine, supported by the use of common standards, procedures and concepts. But given the challenges and opportunities presented by contemporary conflict, joint operations must evolve into more integrated modes of cooperation; what we call multi-domain multi-level (MDML) operations. There is not yet a commonly adopted definition for the term, but the core notion boils down to the significantly improved integration of military forces across the operational domains through a combination of organisational reform and enhanced use of (emerging) technology. It is widely accepted that in many (future) warfighting scenarios, a MDML approach to operations is essential to achieve the multi-level effects necessary to gain a competitive edge over opponents. Indeed,

[81] https://cyberstability.org/wp-content/uploads/2018/11/GCSC-Singapore-Norm-Package-3MB.pdf

MDML operations should not only be seen as a set of aspirations, but as an enduring characteristic of future warfare that will only grow as conflict becomes more complex.

Next level jointness

"Conflicts are increasingly fought simultaneously across the land, air, sea, space, information and human domains, in military next to traditionally civilian arenas. Due to the ever-deeper integration of IT technology, the pace of conflict continues to accelerate while the strategic, operational and tactical levels are further compressed. […] This means that to be effective, armed forces need to be able to coordinate and synchronise actions both horizontally (across the warfighting domains) and vertically (across the levels of war). This has significant implications for the way our armed forces must prepare and organise to prevail in future armed conflict. Existing notions of combined arms and joint operations should be taken to the next level."[82]

The concept of MDML operations deeply influences (the design of) defence planning, force generation and force deployment. Creative thinking is required on how interactions and agreements between the various military branches representing the operational domains should be aligned. Within the context of a military mission, the constituent land, sea, air/space and cyber 'lines of operation' do no longer constitute largely independent series of activities that occasionally interact (with some high-level coordination), but will increasingly be intrinsically interwoven in terms of preparation, planning and execution. How this exactly should be done, is a critical conceptual challenge for the defence organisation for the period up to 2030-35.

Total Force. As already underlined in the previous Chapters, the multi-faceted nature of contemporary security challenges calls for a whole of society approach. The multi-domain approach described above should, mutatis mutandis, be expanded to the civil domain as well. This is sometimes referred to as the 'total force' concept. The 2018 Defence White Paper states that "Organizational agility is vital to improving our ability to respond to the constantly changing security environment". Opportunities for collaboration with, for example, hospitals, educational institutions, and technology companies as well as the increased use of reservists must be developed to be able to deploy more effectively and for longer periods of time. The Norwegian 'Total Defence' concept may provide an example (see text box below).

[82] HCSS, Playing to Your Strengths. A Different Perspective on Future Capabilities for the Royal Netherlands Army, 2018.

Trident Juncture 2018

NATO has always had an important role in supporting and promoting civil preparedness (initially known as civil emergency planning) among Allies. The principle was set out in Article 3 of the NATO Treaty, which requires all Allies to "maintain and develop their individual and collective capacity to resist armed attack". This involved supporting continuity of government, the provision of essential services and civil support to the military. Much of these efforts faded over the last decades, only to get back into focus after Russia's annexation of Crimea and the rise of ISIS. Central to the renewed NATO approach is training and exercise, nationally or in an Alliance setting. Exercise Trident Juncture in October 2018 (TRJE18) enabled Norway to exercise and validate aspects of its approach to societal resilience within its Total Defence concept. Civilian organisations, like the health sector, the Norwegian State Railways, Norwegian Public Roads Administration and the Norwegian Directorate for Civil Protection, participated in hosting the Allied troops during the exercise. More than 50,000 soldiers from 30 countries, 65 ships and 250 aircraft participated. TRJE18 also provided other Allies the opportunity to experience (once again) how comprehensive and joint civil/military exercises can help prepare for the full range of contingencies they could face in light of the current and future strategic environment.

6.3 Accelerating Technology Affects All

The game-changing nature of AI. The rapid developments in Artificial Intelligence affects all Strategic Challenges. Because AI is a general purpose technology - more like the combustion engine or electricity than a weapon - the competition to develop it will be broad, and the line between its civilian and military uses will be blurry.[83] Instead of one military AI arms race, there will be many AI arms races, as countries and violent non-state actors develop or apply new algorithms for military purposes.[84]

There is, however, a possible catch. AI has the potential to become a profound game changer by dramatically speeding-up military decision cycles by pushing humans out of the OODA loop. A recent HCSS report indeed concludes that AI-related technologies may upset the military balance of power and carry the risk of 'hyperwars' as a result of human-out-of-the-loop use cases.[85] Let us spell out these two deeply

[83] According to a McKinsey Global Institute report, in North America the private sector invested some $15 billion to $23 billion in AI in 2016, more than ten times what the US government spent on unclassified AI programs.

[84] Note that most military applications of AI will be a far cry from the killer robots depicted in Hollywood films. For example, computer-run algorithms could aid militaries in effectively training personnel, better logistical planning and operations, improving surveillance and detailed target recognition.

[85] HCSS, *Macro Implications of Micro Transformations. The Geopolitical Causalities of Artificial Intelligence*, forthcoming.

troubling possible consequences. The first is that a state succeeding in strategically harnessing AI to achieve a fundamental leap forward in warfighting capabilities, may choose to reap the benefits from doing so perpetually. This is the 'winner-takes-all' dynamics we see in e.g. Google's search function or Facebook's social media dominance mapped upon the global security environment. A second possible effect is autonomous AI running out of control (see text box). Militaries are unlikely to knowingly field weapons they cannot control, but war is a hazardous environment and requires balancing competing risks. Faced with the choice of falling behind an adversary or deploying a new and not yet fully tested weapon, militaries are likely to do what they must to keep pace with their enemies.

AI and stock and market crashes.

Automated stock trading provides a useful window into the perils of this dynamic. In 2010, the Dow Jones Industrial Average lost nearly 10 percent of its value in just minutes. The cause? A sudden shift in market prices driven in part by automated trading, or what's come to be known as a flash crash. In the last decade, financial markets have started to suffer such crashes, or at least miniature versions of them, on a regular basis. The circuit breakers installed by regulators to pull a stock offline can't prevent incidents from occurring, but they can stop flash crashes from spiralling out of control. Circuit breakers are still regularly tripped, though. For instance, on August 24, 2015, more than 1,200 of them went off across multiple exchanges after China suddenly devalued the yuan.

Humanity stands at the threshold of a new era in war, in which machines will make life-or-death decisions at speeds too fast for human comprehension. Towards the end of the period up to 2030-35 or just beyond, the risks of such a world are likely to become real and profound. The unrestrained pursuit of fully autonomous weapons could lead to a future where humans cede control over what happens on the battlefield. Mitigating measures include the integration of AI into the Dutch Armed Forces' structure on the one hand, and to be better equipped against asymmetric warfare on the other. In a broader frame, AI-related technologies' contribution to conflict escalation can be addressed by increasing barriers to escalation - an area in which international regulations governing systems explainability are of particular interest. Reviewing existing arms control regimes or proposing dedicated new ones, requires the development of a differentiated (shared) understanding of robotic and autonomous systems at the international level on the one hand, and the adoption of standards vis-a-vis systems explainability on the other. But even if all countries agreed on the need to restrain this class of arms, the fear of what others might be doing and the inability to verify disarmament could still spark an arms race. Less ambitious regulations could fare better, such as a narrow ban on anti-personnel autonomous weapons, a set of rules for interactions between autonomous weapons, or a broad principle of human involvement in lethal force. While such modest efforts might mitigate some risks, however, they would leave countries free to develop many types of autonomous weapons that could still lead to widespread harm.

Robotic and Autonomous Systems (RAS) and ethics. (Semi-)autonomous systems have been in operation for over four decades and have previously received relatively limited little ethical consideration. But as systems become increasingly independent, the concern for rogue robots has arisen. The recent ethical debate on RAS has been dominated by relatively extreme narratives akin to banning 'killer robots' (used as a euphemism for all RAS) entirely. This has side-lined nuances and may have critical implications on the further experimentations with and implementation of RAS in a military context. The military must become more involved in the ethical debate on the military use of autonomous systems in order to present a balanced view between the substantive ethical concerns and the inevitable grow of RAS applications (but also with the longer-term spectre depicted in the previous point in mind). The Royal Netherlands Army already works together with TNO and HCSS to feed the public and political debate on the military use RAS. A recent HCSS paper highlights three key ethical challenges arising from the introduction of RAS.[86] These key challenges are 1) *human agency*, the ability of humans to retain control over systems; 2) the ways in which RAS in a military context affect *human dignity*; and 3) the *(human) responsibility* structures for deploying RAS. These challenges provide guidance for informing the 'RAS & ethics'-debate.

Dual-use technology and triple helix cooperation. The increased speed of technological development requires that the rate of innovation of the Armed Forces increases sharply. Innovation must become a central process in the defence value chain. Structural cooperation between government, knowledge and industrial partners is a prerequisite to maintain a high-quality, competitive military that can quickly and easily adapt to a changing security environment. The better the Armed Forces manages its (national) ecosystems with private industry, especially with technology firms, the more likely they are to derive a crucial advantage in future conflicts. However, unlike a stealth bomber which has only military applications, most military relevant technology nowadays has both military and civilian uses. This dual-use character creates an incentive to spread new (applied) technology to global markets, and therefore makes it much harder to keep research classified. Companies can co-opt advances made by market leaders, making it hard to sustain a large first-mover advantage. This reverses the dynamic from the Cold War, when government

[86] HCSS, The Ethics of Robotic and Autonomous Systems in a Military Context, September 2019, https://hcss.nl/report/towards-responsible-autonomy-ethics-ras-military-context

investments led to private sector innovation and produced technologies such as GPS and the internet. This crucial development underpins the requirements for:

- deep cooperation between government, knowledge organisations and industry ('triple helix') over innovation;
- fundamental reform of the defence business processes for specification, development, procurement, commissioning, upgrading and disposal of capacities and systems. Where they now act as a threshold for (fast) innovation, they will have to facilitate innovation;
- ample space to experiment (Concept Development & Experimentation, CD&E) to be able to take meaningful innovation steps quickly. End users must be intrinsically part of experiments;
- organisational measures to ensure that successful experiments can be absorbed quickly in the organisation and possibly scaled up;
- a permanent technology watch & assessment function that performs horizon scans for potentially disruptive new technologies and market explorations for new military-relevant products and services;
- Defence willing and able to act as a smart integrator of commercially available technologies (possibly in the form of services).[87]

[87] Part of a smart integration strategy is to be aware of, and possible mitigate for, technological dependency. Defence organisations have increasingly become dependent on enabling technologies and standards that are developed in and enforced by global civil markets. Underlying supply chains are almost invariably dependent on the international market and not transparent at the lower tiers. This dependency of military supply chains on various actors, e.g. China, leads to major vulnerabilities that should be managed.

***The Hague* Centre for Strategic Studies**

info@hcss.nl

hcss.nl

Address:
Lange Voorhout 1
2514EA
The Hague
The Netherlands