The Hague Centre for Strategic Studies

HCSS SECURITY

Playing to Your Strengths

A Different Perspective on Future Capabilities for the Royal Netherlands Army

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.

Playing to Your Strengths
A Different Perspective on Future Capabilities for the Royal Netherlands Army
HCSS Security
The Hague Centre for Strategic Studies

ISBN/EAN: 978-94-92102-65-2

Authors: Tim Sweijs, Frank Bekkers, Stephan De Spiegeleire.
Contributions by Michel Roelen.

HCSS Project Team: Frank Bekkers, Reinier Bergema, Paula Faber, Karlijn Jans, Lotte de Jong, Mihailo Jovetic, Lucie Kattenbroek, Matthew Phillips, Michel Rademaker, Rob de Rave, Michel Roelen, Stephan de Spiegeleire, Tim Sweijs, Bianca Torossian, Rob de Wijk, Eric Wilms, Eline Wildöer.

Figures 1, 6, 8, 10, 12, 14, 16, 18: Scenarios4Summits

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

Playing to Your Strengths

A Different Perspective on Future Capabilities for the Royal Netherlands Army

Table of Contents

Executive Summary

This report contains the results from a research project aimed at identifying new capabilities for the future Royal Netherlands Army (RNLA). Rather than sketch a full future force profile, it concentrates on promising new, or to be renewed capabilities. The results are intended to feed ongoing transformation efforts within the RNLA and inform the Army leadership in anticipation of the Defense Review 2020 [*de Herijkingsnota*].

In the transition from the Industrial to the Information Age, the RNLA's ability to successfully operate within conflict environments, as well as in the grey zones below the threshold of open conflict, is under pressure. Over the next decade, Dutch armed forces will face adversaries that will deploy a wider range of instruments of violence in various ways in order to attain their political objectives. This will happen in the context of a changing character of armed conflict, due to technological, social, cultural and political developments that spur a cascading process of military-strategic innovation. This process is evolutionary rather than revolutionary in nature, but is likely to feature punctuated bursts of rapid change along the way.

Armed forces need to adapt in order to be able to successfully tackle the challenges in the future conflict environment. Despite all the transformational verbiage of the past few decades, force providers still overwhelmingly procure traditional big-ticket items. This is problematic because of *techflation*, the tendency of military platforms to become ever more expensive. As a result, the armed forces of especially small and medium force providers have seen a massive decrease in the number and the diversity of platforms, leaving them vulnerable both to attrition and to adversaries who can specialize in defeating one type of platform.

In the context of the changing character of conflict on the one hand, and the burgeoning costs of traditional military platforms on the other, force providers should actively explore new capabilities for their armed forces that play to their strengths. For small and medium sized force providers, their agility puts them in a relatively propitious position to pursue innovative concepts and capabilities, instead of trying to merely be smaller versions of the great powers' militaries. They have smaller bureaucracies and units, more direct lines of contact between key stakeholders (both within and outside the armed services) and, given their much smaller defense budgets, have greater incentive to innovate efficiently. Small and medium size force providers can use these features not only to experiment with new concepts and strategies with

the military systems provided by the dominant shapers, but also to develop and adopt new military capabilities that fit well with their national political, economic and societal characteristics. These premises serve as the point of departure for this study.

This report presents six themes, each suggesting a diverse set of new or to be renewed capabilities for the RNLA. These themes were identified on the basis of a multimethod approach, involving desk research, national and international stakeholder consultation, and two half-day scenario workshops conducted with the participation of a hand-picked group of forward-leaning, creative thinkers from within the RNLA. In the scenario workshops, the capabilities required or desired for a set of eleven conflict scenarios were discussed. This process yielded a long list of future capabilities for the Army, which were subsequently assessed according to whether they (1) played to the strengths of the Netherlands; and (2) were sufficiently different from the current incarnation of the RNLA on the basis of *lenses*.

The four *core strengths* for the Netherlands that we identified were:

- **Size**: the Netherlands is sufficiently small to be agile, yet large enough to create sufficient mass and make a difference;
- **Technologically advanced**: the Dutch economy and knowledge landscape is geared toward generating high-quality solutions;
- **Multi- and transdisciplinary**: the Dutch connect relatively easily across different disciplines and institutional stovepipes to create crossover and/or integrated innovations;
- **Connected**: the Netherlands is one of the most globally connected countries and is widely considered a worthwhile (government-to-government and business-to-business) cooperation partner.

We also formulated alternative *lenses* which present different perspectives on the role of the Army:

- The Army as the **Custodian of the Human Domain**. The army is not primarily about fighting (and winning against) other armies, but instead serves primarily as the custodian of the human domain.
- The Army is about the **Influence Chain**. The army is not about the kill chain, but about the (effective, goal-oriented) human influence chain.
- The Army is about **Actionable / Actioned Intelligence**. Physical force is subordinate to cognitive intelligence in terms of achieving defense and security goals.
- The Army as a **Sustainable Security Solution Provider**. Sustainable security solutions are preferred over punctual (hard-fought and probably ephemeral) victories. Thus, the army is about continuous resilience building and prevention as opposed to being response-oriented.

These strengths and lenses were used to identify various capabilities within the following six themes:

1. Rethinking Phase Zero: Shaping the Human Domain;
2. Multi-Domain, Multi-Level Operations;
3. AI in the OODA Loop;
4. Robotic and Autonomous Systems;
5. Mosaic Warfare: Distributed and Networked Capabilities;
6. Empowering the Agents of Resilience.

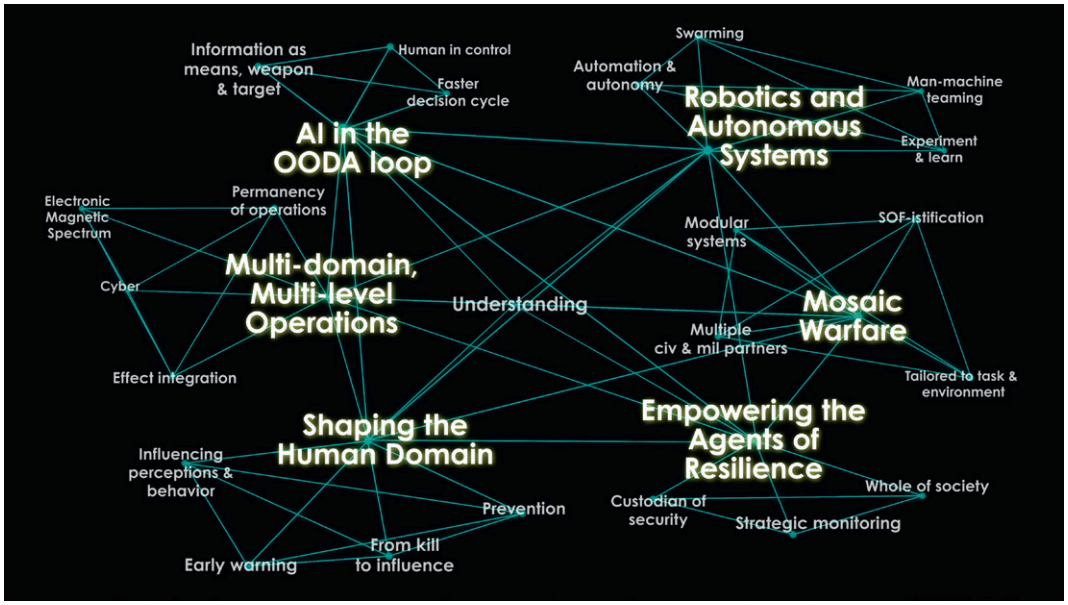

Figure 1: Six connected themes for new or to be renewed future army capabilities

This report offers a concise description of each of these themes, examines relevant developments for the Army, and identifies promising and typically underexplored capabilities or lines of capability development that the RNLA can pursue in conjunction with a particular theme. This is summarized in Table 3 on page 53.

The themes *Multi-domain, Multi-Level Operations* and *Empowering the Agents of Resilience* largely fit within the current notion of the RNLA and point to capabilities that require an intensification and expansion of ongoing efforts rather than to radically different capabilities. Other themes build on developments that have already been set in motion but that are still in their very early days, such as *AI in the OODA Loop* and *Robotic and Autonomous Systems*. Due to their rapid development, the capabilities within these two themes will require significant experimentation against moving targets. Finally, the capabilities identified within the *Rethinking Phase Zero* and *Mosaic Warfare* themes will necessitate considerable expansion of the existing mindset and prevailing practices. The development of these capabilities will require entrepreneurship to get them off the ground and senior level commitment to see them materialized.

It is crucial that the rate of innovation within the Dutch armed forces accelerates, and that the capacity for initiating and guiding these innovation processes is strengthened. This should be done in recognition of the fact that the bulk of innovation stems from the civil sector, and that many technological developments – certainly those at the crossroads where complementary technologies meet – are exponential. This requires new forms of civil-military cooperation and procurement strategies that facilitate continuous innovation. To get things moving, the armed forces should redesign innovation processes and adjust bureaucratic structures by:

- **Scaling from the edge**, by setting up workshops to freely experiment with technology areas that are developing rapidly. In these workshops, suppliers, researchers, developers and end users have room to jointly develop and experiment with new products and concepts. These will serve as test beds for innovations with immediate feedback loops to and from practitioners on the ground.
- **Stimulating adaptation and renewal as a continuous process**. The armed forces need a multi-speed acquisition process with different innovation cycles for platforms and for the systems on those platforms. Platforms (ships, aircraft, vehicles) typically take many years to acquire and have a twenty year plus lifespan. On-board systems (ICT, sensors, shooters) currently run on a similar cycle, which means that they are often outdated even before their first commissioning. This regime has to be replaced with an incremental, plug-and-play approach in which systems are modernized in a modular fashion.
- **Linking innovation to anticipation.** The armed forces need to institutionalize a permanent technology watch and assessment function which conducts long-term horizon scanning of emerging technologies with a potentially disruptive impact, and monitors new military-relevant products and services that come on the market. The latter becomes more important because armed forces seek to become smart integrators that increasingly leverage commercial civil technologies. Technology watch and assessment should be conducted in close association with a general anticipation function that assesses trends, developments, threats and opportunities in the global security environment.

These adaptations of existing processes and structures will greatly enhance the ability of the armed forces to pursue promising new capabilities across the six themes, as summarized in Table 3 on page 53. This, in turn, will enable the RNLA to continue making important contributions to national and international security for the next decade and beyond.

1. Introduction

1.1 The Character of Conflict is Changing, are Military Forces Keeping Pace?

In the transition from the Industrial to the Information Age, the Netherlands Army's ability to successfully operate in conflict environments as well as outside of them is under pressure. Over the next decade, our armed forces will face adversaries that will deploy a much wider range of conflict instruments in different ways to attain their political objectives. This will happen in the context of a changing character of armed conflict. Technological, social, cultural and political developments spur a cascading process of military-strategic innovation. Although this process is evolutionary rather than revolutionary in nature, it is likely to feature punctuated bursts of rapid change along the way.

Figure 2: The changing character of conflict and the future battlespace

In recent years, contemporary conflict actors are competing more explicitly across the physical land-sea-air domains as well as the cyber and the human domain.[1] They employ a mixture of conventional and unconventional means, in grey zone conflicts that stay below the threshold of war (e.g., the dispute between Russia and the West),

1 With air increasingly extending into space which, despite international treaties, is almost inevitably on a trajectory towards militarization; and cyber including the information and the electromagnetic spectrum.

as well as in proxy conflicts that feature high levels of violence (e.g., Syria and Yemen). State actors are rebuilding and modernizing their traditional, kinetic weapon arsenal at the same time as they actively explore non-kinetic instruments to gain strategic advantage over competitors. The 'weaponization of information' by the Russian government and its manipulation of societal discourses in Western democracies through the exploitation of social media platforms is one example.[2] The ability of ISIS to mobilize thousands of foot soldiers from across the globe through sophisticated social media marketing campaigns, and to coordinate attacks from afar, shows that this is certainly not the prerogative of states. The battle for the hearts and minds has moved out-of-theatre and is now being waged in the human domain that transcends national boundaries.

Over the next few years, advances in robotics and unmanned systems (RAS) and artificial intelligence (AI) are expected to further affect the ways in which actors wield weapons for political purposes. The proliferation of unmanned systems is progressing speedily. By the latest count, 28 countries have already developed or acquired armed unmanned aerial vehicles.[3] Unmanned systems are slowly making inroads in the land domain too. Although few unmanned land platforms are used in current operations, this is expected to change soon.[4] Unmanned systems are certainly not exclusive to state actors. Non-state actors such as ISIS in Syria and Iraq, the Houthi Rebels in Yemen and Hezbollah in Lebanon, have already used unmanned vehicles to launch aerial and naval attacks. More generally, off the shelf technology – the type that can be purchased at tax free shops in airports – can now be weaponized relatively easily, also by non-state actors with low levels of organization.

Alongside the ongoing revolution in RAS, major powers have begun to appreciate the importance of AI to boost their military capabilities. Not long ago, Chinese military strategists coined the notion of 'intelligentized warfare', undoubtedly inspired by the 'informatized warfare' waged by the US since the early 1990s.[5] China, Russia and the US have been ramping up expenditures on military applications of AI. They have established AI cells at the center of their military establishments to harness and unleash the power of this potentially revolutionary enabler. Current efforts predominantly focus on doing traditional things smarter. This includes the automated analysis of imagery or more rapid target acquisition – initiatives that are typically aimed at shortening the OODA loop (Orient – Observe – Decide – Act), or at making

2 Hansen, "The Weaponization of Information"; Waltzman, "The Weaponization of Information."
3 And also by most recent estimates, 31 countries are in possession of ballistic missiles. Arms Control Association, "Worldwide Ballistic Missile Inventories"; Bergen et al., "World of Drones, Examining the Proliferation, Development, and Use of Armed Drones."
4 The Russian government for instance has openly announced its intention to make 30% of its land platforms unmanned by the year 2025. See Bendett, "Red Robots Rising"; Gady, "Meet Russia's New Killer Robot."
5 Kania, "Battlefield Singularity."

it more efficient otherwise.[6] But it is unclear what capabilities are being developed behind closed doors and what their impact will be on the character,[7] perhaps even the nature,[8] of armed conflict. What *is* clear, is that the 'future of violence' is emerging more rapidly than many of us anticipated only a few years ago.[9]

1.2 Transformational Talk and Techflation

It is widely acknowledged that armed forces need to adapt in order to be able to successfully tackle the challenges in the future conflict environment. In fact, few observations are as popular throughout the defense foresight and planning communities as those asserting exponential change. Yet, despite all of the transformational verbiage of the past few decades, force providers still overwhelmingly procure traditional big-ticket items, such as jet fighters for our air forces, frigates for our navies, and armored personnel carriers and artillery pieces for our armies. In other words, armed forces, similarly equipped as they have been for decades, are expected to perform more or less the same activities in the future as in the recent past and the present, with an only slightly enhanced capability portfolio.

This is made more problematic because of *techflation*, a term denoting the tendency of military platforms to become ever more expensive.[10] As a result, the armed forces of especially small and medium force providers have seen a massive decrease in the number and the diversity of platforms (for a comparison of the major platforms of the Dutch Army, 1990-2018, see Table 1).[11] Even though they still possess technologically highly advanced platforms, it has left them – paradoxically – more fragile for two principal reasons. First, the paucity in numbers leaves them particularly vulnerable to attrition. Second, the lack of diversity in platforms means that adversaries can develop capabilities singularly aimed at defeating that one type of platform. In the context of deep uncertainty and a rapidly changing environment, uniformity is generally considered a weakness rather than a strength.[12] We may soon be nearing the 'end of the line', a moment in time at which smaller and medium force providers can simply no longer afford next generation technology.[13]

---

6 De Spiegeleire and Sweijs, "Artificial Intelligence and the Future of Defense."
7 Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power."
8 Hoffman, "Will War's Nature Change in the Seventh Military Revolution?"
9 With some exceptions, see for instance Wittes and Blum, *The Future of Violence*.
10 See Norman R. Augustine, an American Army under Secretary from 1975-1977, who famously asserted that 'In the year 2054, the entire [US] defense budget will purchase just one aircraft. This aircraft will have to be shared by the Air Force and Navy 3-1/2 days each per week except for leap year, when it will be made available to the Marines for the extra day.' See Smallwood, "Augustine's Law Revisited."
11 See Scharre, "Robotics on the Battlefield Part II."
12 Paul Davis on FAR principles: see e.g. Davis, "Lessons from RAND's Work on Planning Under Uncertainty for National Security."
13 Søby Kristensen, "Military Technology and Small State Strategies.", presented at the Seminar 'Navigating new military technologies: small state strategies for maintaining relevant and effective military forces' hosted by Defence Command Denmark in Slagelse, Denmark on 22 May, 2018.

Units / platforms	1990 total	1990 combat ready	1990 mobilization	2018 total
Mechanized infantry battalions	19	10	9	2
Infantry fighting vehicles	2889			141
Air mobile infantry battalions	0			3
Motorized infantry battalions	0			2
Tank battalions	12	5	7	1/3
Tanks	913			17
Artillery battalions	20	13	7	1
Artillery systems	481 (4 types of systems)			18 (1 type of system)

Table 1: Decreasing numbers of units and main weapon systems of the Dutch Army between 1990 and 2018[14]

From the perspective of a prudent military planner, this offers an additional reason to complement the currently dominant *legacy based planning* approach to future force planning with a view of identifying different *future* capabilities that are both effective and affordable. In the context of the changing character of conflict on the one hand, and the burgeoning costs of traditional military platforms on the other, small and medium force providers should actively explore new future capabilities for their armed forces which play to their strengths. Their relative agility puts them in a propitious position to pursue new capabilities, instead of trying to merely be smaller versions of the great powers' militaries.[15] They have smaller bureaucracies and units, more direct lines of contact between key stakeholders both within and outside the armed services and, given their much smaller defense budgets, greater incentive to innovate. Small and medium size force providers can use these features to not only experiment with new concepts and strategies with the dominant military systems provided by the dominant shapers, but also to develop and adopt new military capabilities that fit with their political, economic and societal profile as a nation. These premises are the point of departure for this study.

1.3 This Study: Future Capabilities for the Netherlands Army

The Royal Netherlands Army (RNLA) has asked *The Hague* Centre for Strategic Studies (HCSS) to conduct a study about new potential capabilities for the RNLA with a time horizon of some ten years and beyond into the future. This report is the result of that study. It does not seek to sketch a full future force profile. Instead, it focuses squarely at promising new or to be renewed capabilities. The results are intended to feed into

14 Ministerie van Defensie, "Eindrapport Verkenningen 2010 Houvast voor de krijgsmacht van de toekomst."
15 In the business world, for instance, market leaders often have trouble maintaining a consistent culture of innovation, while smaller companies are better at fostering innovation.

the Army leadership's deliberations about their input to the Defense Review 2020 [*de Herijkingsnota*] (see Textbox below), as well as inform the ongoing transformation efforts within the RNLA.

Dutch Defense Expenditures and the Dutch Defense White Paper 2018

The Dutch armed forces just emerged from over a quarter century of budget cuts. In 2015, with 1.14%, Dutch defense spending as percentage of GDP hit its lowest point in two centuries. From values close to 2.5% in the 1980s, it has entered a steady decline since 1993 with values below 2%. Since 2015, the percentage crept up slowly to 1.23% in 2017.

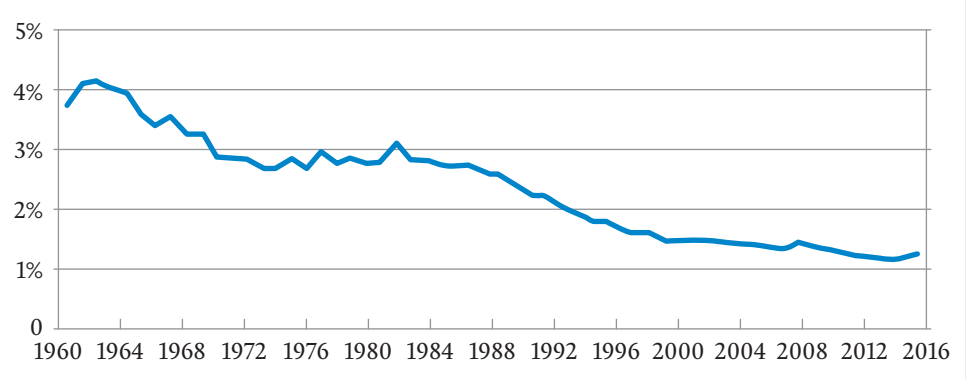

Figure 3: Dutch Defense expenditures as percentage of GDP[16]

As a result of years of cuts, the Dutch Armed Forces exhibit low levels of operational readiness, considerable wear and tear of existing systems and depleted ammunition stocks, while morale amongst the uniformed personnel has suffered. However, the Arab Spring that turned into Winter and Russia's aggressive behavior epitomized by its Annexation of Crimea and the shooting down of the MH17, with 196 Dutch citizens aboard, marked a turning point. A political consensus emerged in which most political parties support a larger defense budget, initially only by partially reversing previously announced defense cuts, but followed more recently by investing an additional € 1-1.5 billion per year. The Dutch Defense White Paper that was published in March 2018 put the modernization of the Dutch armed forces central but was more about rebuilding, upgrading and replacing and modernizing the legacy force than it was about reinventing the new one.[17] The program outlined in the 2018 White Paper will be revisited in the 2020 *Herijkingsnota*.

16 Based on data of the Stockholm International Peace Research Institute (SIPRI). SIPRI uses data derived from the NATO definition, which include all current and capital expenditures on the armed forces. Other definitions render slightly different percentages, but showing the same trend. See e.g. Dijsselbloem, "Toezegging debat Najaarsnota 2015: Defensie-uitgaven."

17 Ministerie van Defensie, "Defensienota 2018: Investeren in onze mensen, slagkracht en zichtbaarheid."

This report proceeds as follows. Firstly, our methodological approach will be described and rationalized in Chapter 2. Chapter 3 will then detail a number of new or to be renewed capabilities or lines of development clustered under the six previously discussed themes. Chapter 4 will summarize our findings and offer some concluding remarks.

2. A Word on Method

2.1 The Concept of a Future Force

The aim of the study is to identify new or to be renewed capabilities for the Army's future force. In order to explain our approach to meet this study objective, we first must look at what we understand by the term 'future force'.

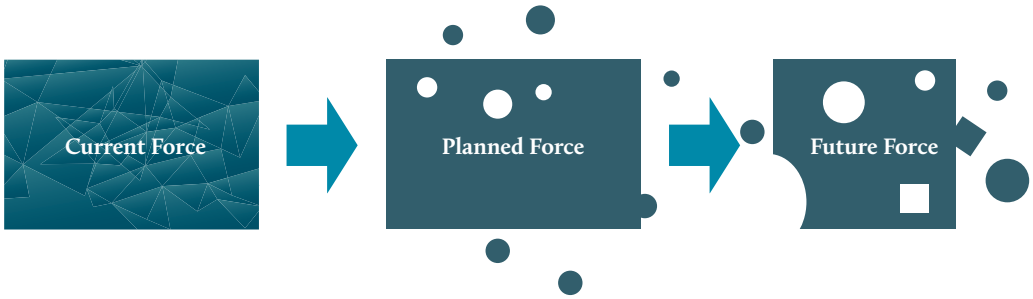

Figure 4: Traditional way of thinking about future capabilities

Figure 4 illustrates the way in which most defense planners still think about forward capability planning. On the left side of the picture, we see the **current force**, which represents a country's current capability portfolio – its armed forces.[18] The current force is figuratively depicted in Figure 4 as a box and a single color to indicate that it is clearly bounded. It is the result of a variety of force element choices that have been made in the past and have led to the force as it exists today. The current force has strengths and weaknesses. Some of these have been exposed in actual operations, while others result from newly emerging threats and opportunities, and still others have to do with changing expectations of the role of the armed forces. Planners want to preserve the strengths and address the weaknesses.

This brings us to the second box in Figure 4: the **planned force** or the objective force. This is typically an incremental improvement of the current force into a still mostly similar force, taking into account the more or less fixed investment programs that have been agreed upon in the defense budget and planning cycle. In our visual depiction of it, the basic parameters of the force remain the same: it is still a rectangle and it is still green. But the fractures we saw in the current force have

18 The current force is obviously not static – it constantly evolves and is being optimized. But for the purposes of our stylized description here, we may think of the current force as a steady-state construct that represents the force as it exists.

now been removed (at least aspirationally) and some force elements may have been shed and replaced by others, which appear (slightly) outside of the box. These new force elements, however, tend to be mostly kind-for-kind replacements of existing systems, whereby a new technologically improved version of an existing weapon system replaces an older version of the same category (e.g. a fifth generation jet fighter replacing a fourth generation one). There may be exceptions to this rule whereby, for instance, unmanned combat aerial vehicles start getting rolled out in the force; but all in all the fundamental shape of the force is not altered by these changes.

The third box in Figure 4 is the **future force**: a vision of longer-term capability priorities. In the prevailing view of forward defense capability planning, the future force is often still envisaged as some sort of further evolution of the planned force, even if slightly more aspects of it are open to change. As depicted in Figure 4, the future force is still, in essence, a green box. Compared to the planned force however, we do see some differences. Indeed, it is more uncertain (in this case more opaque in color), its shape could be slightly reoriented, the color might be a somewhat different shade of green; more elements could be replaced – and not merely kind-for-kind, but also by truly different capabilities. Still, in this way of looking at the three time horizons, the future force is essentially still a further derivative of the planned (and thus also the current) force.

This incremental way of looking at future force development may be sufficient in periods of slow change and/or when organizations are essentially satisfied with their recent and current performance. However, our own assertion is that neither of these conditions are currently met. We therefore submit that the incremental approach that lies at the heart of our current thinking about forward capability development carries enormous risks.

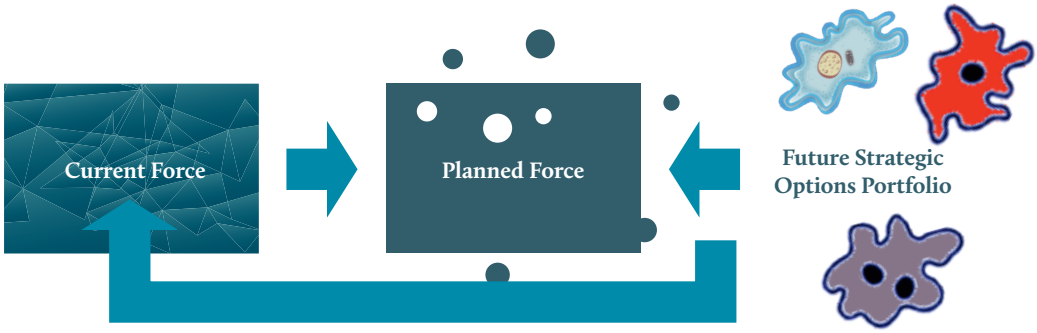

Figure 5: Alternative way of thinking about future capabilities

Figure 5 suggests an alternative, but also complementary, way of thinking about future capabilities. This approach still retains the *planned force* construct that is derived based on a 'left-to-right' logic. But it adds a 'right-to-left' *future force* planning effort in which not the current force (assets / organization / processes / mindset

etc.) and how to improve it is the determinant of future efforts, but different, new force elements that are elicited from a number of different angles. To illustrate the differences between the planned force construct and this future force construct, Figure 5 visualizes the force elements not as circles or rectangles, but as amoeba-like polygons in different colors. Another important difference is that this future capability portfolio is not depicted as a single force (box), but as a rich portfolio of different force options. As the future space becomes more discernible, this strategic options portfolio will constantly have to be adjusted and updated – but the idea is that it has to be diversified enough to enable a defense organization to 'get there early'.[19]

Whereas the planned force is best served by analytical rigor (with a healthy element of creativity), the future options portfolio primarily demands creativity (with a dose of analytical rigor). The main driving question here should not be how to improve the current force. Instead, it should be how to ideate different force elements that still represent 'force', but are more about what we can do to achieve our security objectives with ways and means that would be very different from the ones that we have today. If in the process of trying to think up such new force portfolio options designers (and not just planners anymore) identify new creative force options that are still widely deemed to be potentially very useful in the short to medium term, these could still be fed immediately into the current force or into the current investment plan. However, the primary driving force behind this particular effort is not this, but rather to try and generate creative new ideas to achieve our security objectives.

2.2 General Set-up of this Study

With the above interpretation of future force in mind, our study approach involved pursuing different avenues to stimulate creativity, while at the same time maintaining an analytical structure that progressed towards a focused end product. These different avenues were not so much parallel, stand-alone exercises, but rather largely consecutive efforts with the results of one avenue feeding into the next, as briefly described below.

2.2.1 Military-Strategic Challenges

To start with, based on a literature review, we identified a set of military-strategic challenges that are generally considered to be important in the future security environment. These military-strategic challenges were presented at various fora, including the senior leadership course of the Dutch armed forces.[20] In addition, we solicited the views of recently retired senior military practitioners on what they consider important future capabilities for the Dutch armed forces as a whole. We also

19 Johansen, *Get There Early*.
20 Sweijs, "Thinking About the Future of Armed Conflict.", presented at the Senior Military Leadership Course hosted by the Netherlands Defence Academy, on 22 March, 2018, The Hague, the Netherlands.

engaged in a series of online and face-to-face interactions with military force planners from small, medium as well as large size countries including Australia, Denmark, and the United States, to gauge their views on emerging capabilities for their armed forces and identify what may be relevant for the Dutch context.

2.2.2 Future Conflict Scenarios

These military-strategic challenges were used as the basis to create eleven future conflict scenarios (see Table 2). Each scenario describes the context, challenge and principal actors, and outlines a series of political and military strategic objectives for the Dutch armed forces to achieve. To ensure that these scenarios represent a variety of conflict settings, we selected topics that covered various aspects of the possible future conflict space by including a variety of actors, domains, instruments, and demands. We further cross-checked the scenarios against different task and capability lists, including the three constitutional tasks of the Dutch Armed Forces,[21] the NATO Essential Operational Capabilities, the three strategic challenges from the Dutch *Integrated International Security Strategy 2018-2022,*[22] the *National Risk Profile 2016*[23] as part of the *Dutch National Security Strategy* and the security themes from the *Dutch Defense White Paper 2018.*[24]

	Scenario title	Content
1	The Kingdom Calls	Venezuela threatens Dutch overseas territories
2	The Toll of the New Silk Road	Digital and physical flows in the Balkans under threat
3	The Thirty Years War	Burkina Faso as a failing state and spillover to Europe
4	Paralysis at Home	Responding to infrastructure-targeted cyber attacks in the Netherlands
5	The New Cold War Heats Up	Military crisis on NATO's eastern border
6	Back to the Future	Conventional interstate warfare in Eastern Europe
7	Anarchy in the EU	Violent secessionist movements across Europe
8	Hybrid Challenges in a Frontline State	Estonia under direct and indirect threat
9	1953 Redux	Large-scale floods in the Netherlands
10	Moving Upstream: Pre-empting Conflict and Instability	A technology-based multi-stakeholder approach to peace
11	Dreadnought 3.0: Blast into the Future	The future of war is now: disruptive innovation tilts the military balance of power

Table 2: Future Conflict Scenarios

21 Nederlandse Grondwet - Artikel 97: Krijgsmacht.
22 Ministerie van Buitenlandse Zaken, "Integrated International Security Strategy 2018-2022."
23 See The National Network of Safety and Security Analysts, "National Risk Profile 2016: An All Hazard Overview of Potential Disasters and Threats in the Netherlands."
24 Ministerie van Defensie, "Defensienota 2018: Investeren in onze mensen, slagkracht en zichtbaarheid."

These future conflict scenarios were then used during two half-day scenario workshops and were complemented by two online exchanges attended by professional subject matter experts from the Dutch Army. In total, seventeen officers from the Army, with backgrounds in technology and innovation, cyber, simulation, command and information systems, civil-military cooperation, diplomacy, sensoring, defense planning, the human domain, leadership, and military history, took part in the workshops. The participants were selected because they represented the forward-leaning, creative, out-of-the-box thinkers within the RNLA. They were engaged in an in-depth discussion of the future conflict scenarios to identify new or to be renewed future capabilities, with the basic format to phrase a capability being "the ability to <*ends: be able to do something, cause an effect*> by <*ways: a method, approach, concept of operations*> with <*means: particular types of asset*>".[25]

The resulting list of capabilities was very rich, but also quite varied in terms of level (strategic-operational-tactical), innovativeness (truly new versus largely existing capabilities that need strengthening), specificity (the scenario context giving a particular flavor versus more generic capabilities) and elaboration (of ends, ways and means).

2.2.3 Thematic Approach

Most of the available time in the two workshops was dedicated to scenario-based discussions. However, in order to stimulate thinking from different perspectives, the final session of the second workshop was devoted to revisiting the capabilities generated within the context of the eleven future scenarios through the lens of a number of recurring themes during the workshop discussions. These themes were roles (of the armed forces / army); technology insertion; human and/versus machine; optimizing the human factor; information as the key source of power; new forms of deterrence; flows security; and 'the mother of all capabilities': adaptiveness as a fundamental characteristic in a dynamic and uncertain security environment. The results of this final session were processed in the list of capabilities.

2.3 Rethinking and Restructuring the Outcome of the Workshops

2.3.1 Six Themes for New Capabilities for the Netherlands Army

As mentioned, the participants in our workshops were hand-picked to represent forward-leaning, creative thinkers within the RNLA. Because of this conscious choice, our deliberations with them did yield a number of unorthodox, stimulating, and even dissenting views and capabilities that went well beyond those of most similar national and multinational exercises. At the same time, in our analysis, most of the capabilities

25 As a clear-cut way of organizing these capabilities, we used NATO's *Main Ability Areas*: Prepare, Project, Engage, Sustain, C2, Protect, and Inform. These come from NATO, "Framework for Future Alliance Operations."

that were identified in the workshops still tend to derive from *one* particular view of looking at the (future) world and at our (also future) selves.

Some of the most striking characteristics of this 'current Army lens' include:

- 'we' means 'just us' (within the box);
- we are about fighting and winning;
- we are primarily enemy-centric;
- we think in predominantly manned systems;
- we are (and will always be) more about the physical domains than about the virtual ones (information and human domains);
- we are *can do* troubleshooters;
- we are about operations.

Furthermore, in most of the discussions a particular national focus was lacking.[26] In the aftermath of the workshops, the HCSS team therefore decided to take yet another avenue. With the long list of capabilities as a foundation, we came up with a number of themes that, in our view, highlight the most relevant new, or to be renewed, capabilities and/or lines of development.[27] In the selection and formulation of these themes, which form the organizing principle for Chapter 3, the core Chapter of this report, we were inspired by two angles:

- by what we consider key strengths of the Netherlands and (therefore) of the Dutch Army (in order to come up with capabilities where the Netherlands can make a difference); and
- by some unconventional ways – what we may call lenses – of looking at the nature of Armed Forces, thereby attempting to give some counterweight to the current Army lens.

These two angles are elaborated upon in the sections below. We dubbed the resulting six distinct but connected themes that stimulate thinking about new or to be renewed capabilities in Chapter 3 as follows:

1. Rethinking Phase Zero: Shaping the Human Domain;
2. Multi-Domain, Multi Level Operations;
3. AI in the OODA Loop;
4. Robotic and Autonomous Systems;
5. Mosaic Warfare: Distributed and Networked Capabilities;
6. Empowering the Agents of Resilience.

---

26 This was driven by the nature of most of the scenarios, that required EU / NATO / international coalition responses rather than predominantly national actions. Therefore, the discussions focused more on capabilities required for the alliance or coalition as a whole, rather than on the particular contributions the Netherlands Army could make to these international efforts.

27 One of the defining characteristics of this time and age is that the distinction between capability development, acquisition (either as product or as a service) and actual operational use is fading. The notion of 'full development' gives way to an approach of enduring, sometimes rapid, open-ended adaptability.

2.3.2 Playing to Your Strengths

What are the political, economic and societal strengths of the Netherlands as a nation that may be leveraged to develop innovative capabilities for an effective future land force that, from within an international perspective, contribute to particular niches in which the Dutch armed forces can make a relevant and effective contribution to national and international security?[28]

First of all, let us consider size. Within the EU, the Netherlands is often called the smallest of the larger nations and/or the largest of the smaller nations. Small in geographical size, its main ports Rotterdam harbor, Amsterdam Internet eXchange and Schiphol are respectively ranked number one, two (after DE-CIX) and three (after Heathrow and Charles de Gaulle) in Europe. With just 0.23% of the world's population,[29] the share of Dutch exports in world trade in 2017 was 3.2%.[30] With its strong transatlantic ties and solid position within the EU and NATO, the Netherlands is seen by the US as a vital gauge as well as stepping stone for its relationship with Europe.[31] Within the EU, the Netherlands is often viewed as a thought leader for smaller nations to (counter-)balance the power of the large member states. This suggests that innovative initiatives taken by the Netherlands Army could well set the stage for likewise partners to follow – possibly creating a multiplier effect.

Second, the Dutch economy is diversified, robust and technologically advanced. Its population and, by extension, labor force are highly educated. Dutch society is future-oriented and open to change, with an academic culture that stimulates inquisitiveness, curiosity and open minds. As a result, the main trust of Dutch society, supported by government policy, is towards a knowledge economy build upon constant innovation and learning. The Netherlands invariably features in the top-10 of various global innovation and competitiveness indices, and often in the top-5.[32]

Third, the Dutch tend to be quite good at transcending stovepipes and working across different disciplines. In its report *Naar een lerende economie* (2013), the Scientific Council for Government Policy (WRR) underlined that innovation often results from circulating and absorbing existing knowledge across scientific or technology areas and application domains. In many cases, it is not necessary for a country to top the world

---

28 In particular if these niches are identified as shortfalls by NATO or the EU. Although European and alliance capability gaps are derived from the planned forces of member states, they may also inform future force discussions. In a general sense, Dutch strengths such as 'high-tech', 'well integrated' and 'well connected' tend to play into these international capability gaps.

29 "The World Factbook — Central Intelligence Agency."

30 "StatLine."

31 See e.g. the (wiki-leaked) US embassy cable from (then) Ambassador Clifford Sobel that begins as follows: "With the EU divided and its direction uncertain, the Dutch serve as a vital transatlantic anchor in Europe. As one of the original six EU members, the Dutch ally with the British to counter Franco-German efforts to steer Europe off a transatlantic course. The Netherlands' solid European and international credentials create a powerful "multiplier" effect." See US embassy, "US Embassy Cables."

32 E.g. The Netherlands ranked no. 4 in the World Economic Forum Global Competitiveness Index 2017 and no. 3 in the Global Innovation Index 2017 of the World Intellectual Property Organization.

science rankings, as long as it understands developments in science well enough, is connected to networks in which new knowledge circulates and its people have the ability to absorb new knowledge quickly and make it productive. This requires multi- and transdisciplinary connections and approaches, which comes relatively easy to the Dutch. Geographical proximity due to its small size, a pragmatic ethos amongst its people, an egalitarian society, and a political culture of consultation and compromise (the *poldermodel*) are all partial explanations for this. The Dutch government, although certainly stovepiped as most other governments are, also fosters interdepartmental exchanges and consultation bodies.

Fourth, with its historic orientation towards global trade, in combination with a spirit of openness, consultation and pragmatism, the Netherlands is part of, and embedded in, an impressive array of bilateral, multilateral and international cooperative agreements, organizations, structures, processes and projects. The Netherlands topped the DHL Global Connectedness Index 2016 and furthermore, previous HCSS research for the Dutch Foreign Relations Index and the Global Geodynamics Monitor shows that, by and large, nations across the world enjoy close relations with the Netherlands and look relatively favorably upon the country.[33]

Figure 6: The Netherlands is one of the most connected countries in the world

In summary, in terms of its ability to innovate societal structures and processes, and in our case, to adapt the defense capability portfolio in accordance with the changing character of conflict, the Netherlands should leverage these strong points:[34]

33 De Spiegeleire and Sweijs, "Volatility and Friction in the Age of Disintermediation: HCSS StratMon 2016-2017 Annual Report," 31–37; Sweijs et al., "Dutch Foreign Relations Index."

34 Note that (relative) weaknesses of Dutch society may also shape the type of defense capabilities that fit the Netherlands. For instance, the combination of an aging society with a shrinking pool of new labor market entrants, and greater risk-adversity prevailing in society, may for instance support the case for a less labor-intensive future army that relies more on automation and autonomous systems.

- **Size**: the Netherlands is sufficiently small to be agile, yet sufficiently large to create sufficient mass and make a difference;
- **Technologically advanced**: the Dutch economy and knowledge landscape is geared towards generating high-quality solutions;
- **Multi- and transdisciplinary**: the Dutch connect relatively easily across different disciplines and institutional stovepipes to create crossover and/or integrated innovations;
- **Connected**: the Netherlands is one of the most globally connected countries and is widely considered a worthwhile (government-to-government and business-to-business) cooperation partner.

2.3.3 Multiple Lenses

Humans are not just rational decision-makers. Human intuition and emotion deeply affect the choices we make. One of the underappreciated aspects of this process is the importance that frames play in our thinking and choosing, and the role that social construction plays in these frames.[35] Here, we use the metaphor of *lenses* for these different frames. The analogy is with the idea that while we think we see reality with our own eyes, in actuality, this is merely our perception. Indeed, although we experience the illusion of receiving high-resolution images from our eyes, what the optic nerve actually sends to the brain is just a series of outlines and clues about points of interest in our visual field that our brain then assembles into a mental picture. It is hard for us to imagine how other biological beings with different types of eyes see the very same world that we see – like flies whose compound eyes have thousands of individual visual receptors that must create a mosaic of small visual segments that their brains then reassemble into something that is useful for them; or starfish, who have (almost invisible) eyes at the end of each arm that seem only capable of sensing lightness and darkness.

What we can more easily understand, however, is how we can use other lenses, like glasses or microscopes, to correct or amplify our human vision. We can also use sensors to take in aspects of reality that our eyes or our other sensory organs cannot naturally apperceive, such as night goggles, lenses for multispectral imaging or radars/lidars with wearable haptic feedback systems. All of these give us very different perspectives on our surroundings and may lead to different choices or actions.

Besides these physical lenses, there are social lenses that may be equally important in our appreciation of reality and that we learn from our peers. There is a rich literature on these social frames and how they affect our interactions with each other and with our environment. These lenses create frames that are shared schemas of

35 Kahneman and Tversky, *Choices, Values, and Frames*.

interpretation, a collection of shared views, experiences, perceptions and stereotypes that individuals rely on to understand and respond to events. Just as we increasingly no longer rely solely on the lenses in our biological eyes to apperceive the world around us, so too do we want to explore whether and how we should also augment our default social lens through which we perceive and assess the army and its environment with other frames that may shed a different light on (our perception of) reality and the role (missions, tasks, capabilities) of the army within it.

Figure 7: Multiple lenses, seeing different things with different lenses

Below, we have formulated a number of alternative lenses through which we can look at the same reality of current or future contests of wills between political actors, and at the *raison d'être* and core competencies of modern-age armies. We do not claim that these different lenses are either exhaustive or mutually exclusive, and indeed, many more different lenses can be constructed to guide creative thoughts about the future (land) force. But these are the dominant ones that have inspired the choice and formulation of the themes used to structure, select and devise the future capability options and lines of development presented in Chapter 3. These lenses are:

> ***The Army as the Custodian of the Human Domain.*** *The army is not primarily about fighting (and winning from) other armies, but instead serves primarily as the custodian of the human domain.*

Humans do not live in the air or on the seas, but on land. If we look at our national security efforts and capabilities, it is striking that the land component plays a much

bigger role there than its peer services. Much of that has to do with (the lack of) distance, as both tactical and strategic transport in expeditionary settings can often not be conducted efficiently (or safely) over land. But much of it also has to do with the fact that we would never allow our armed forces to use the coarse forms of physical violence at home that we use abroad.[36] Furthermore, land forces are suited for much more discretionary and fit-for-purpose activities than maritime and air forces, especially in our urban environments. This is what land forces should specialize in: subtle forms of violence and non-violent influencing operations, leaving the use of massive destructive power aimed at the opponent's military power to their peers. Note that there is still a sound argument to be made for having armies (as opposed to expeditionary policy or constabulary forces), in order to guarantee both our defensive capabilities and, where possible, escalation dominance in the higher ranges of the conflict spectrum.

> ***The Army is about the Influence Chain.*** *The army is not about the kill chain, but about the (effective, goal-oriented) human influence chain.*

Armed forces represent the sharp cutting edge of our societies' power instruments. They have an extraordinary license, even under international law, to apply instruments and methods of physical violence that we do not tolerate or condone elsewhere. There is, however, some evidence of diminishing returns to scale in applying raw physical violence. In places from the West Bank to Syria to Afghanistan, this has not necessarily led to achieving the objectives of the initiators of that violence. At the same time, we see some tell-tale signs of the increased effectiveness of non-physical violence, where agents of conflict (radical Islam, Russia, etc.) have been able to leverage social media to mobilize their own ecosystems into effective action. In extension of *The Army as the Custodian of the Human Domain*, Western defense organizations, in particular armies, should find more responsible ways to do something similar, in order to start influencing both the conflict *and* the resilience sides of security. The modern-day equivalent of the military's 'legal exceptionalism' should shift from being allowed to kill (if, and only if, certain critically important criteria are met) to being allowed to violate prevailing privacy norms 'for the greater good' (again if, and only if, certain critically important criteria are met).

36 That has even been the case in some recent cases of extreme security challenges. Terrorism has prompted many - also European countries - to once again 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 did not employ heavy artillery.

The Army is about Actionable / Actioned Intelligence. *Physical force is subordinate to cognitive intelligence in terms of achieving defense and security goals.*

The physical destructiveness and lethality of armies is on a declining slope. The largest artillery shells ever used had a caliber of 800mm. Developed by the German Krupp concern in the late 1930s, they were fired out of super-railway guns. The super-sized caliber shells from the two World Wars then gave way to the age of rockets, guided missiles, and bombs, which typically ended up in the arsenals of other services. Today, all modern armies use shells with a caliber between 105 and 155 mm. The few countries that produced nuclear artillery after WWII (France, the Soviet Union and the United States – the UK never put them in production) had by the early 90s, replaced them with mobile tactical ballistic missile launchers, carrying missiles with nuclear warheads, which again ended up in the other services. The RNLA abandoned nuclear artillery in 1992.

The declining lethality of the land component is also visible in the amount of military or civilian casualties of physical military violence. For much of human history, most casualties were undoubtedly inflicted by land forces through direct physical contact. As various forms of projectiles advance in distance, lethality, ease of use and precision, indirect forms of lethality increase in importance. It is only when artillery became explosive in the industrial age that casualties inflicted by the other components started rising dramatically, with armies bearing the brunt of battle casualties received.[37]

The digital revolution is currently changing the balance of power from atoms to bits. A new (armed?) force is digital and not atomic in nature, although it does still require physical assets to survive. Armies now need to be at the edge of the knowledge revolution. The state of the art is highly unlikely to be located within government, and maybe not even in the academic world. Instead, we are seeing this edge shift to the private cumulative knowledge builders (Google, Microsoft, IBM, etc.) *and* in the new open source cumulative knowledge builders (DBpedia, Open Linked Data, etc.). The knowledge graphs that these (oversized) players are building are no longer just about knowledge, but about nudging human behavior to act in certain, algorithmically defined, ways. This may mean that an unusually intelligent or highly skilled, physically handicapped person might be more desirable as an army soldier than a physically fit, but cognitively average person. And, since algorithms are starting to outperform humans in many cognitive (and physical) skills, in the somewhat longer term well-designed learning AI-systems may be the best candidates to apply for many essential military jobs.

37 United Kingdom Ministry of Defence, "Deaths in the UK Regular Armed Forces: Annual Summary and Trends over Time 1 January 2008 to 31 December 2017"; DeBruyne, "American War and Military Operations Casualties: Lists and Statistics."

***The Army as a Sustainable Security Solution Provider**. Sustainable security solutions are preferred over punctual (hard-fought and probably ephemeral) victories. Thus, the army is more about continuous resilience building and prevention as opposed to being response-oriented.*

For most of recent history, we have had no alternative but to use our armies in responsive ways. Our actionable fine-grained evidence on what was actually happening in the world, let alone the deeper patterns behind it, was extremely limited. Armed forces understand better than anybody else the tremendous human (physical and psychological), materiel, financial and political costs of the application of (preferably massive and overwhelming) violence of these responsive deployments and engagements. But our knowledge and understanding of our (human) environment is rapidly expanding and offers the possibility to actively pursue 'sustainable' security solutions that detect rising tensions early in the process and prevent escalation into (open) conflict. A medical analogy is that, through a vastly better understanding of the human genome and physiology, personalized medicine and medical treatment is used to prevent diseases rather than trying to cure it.

In achieving sustainable solutions, the security ecosystem is crucial. As the primacy of Westphalian borders has been challenged and the power of traditional nation-states has been waning over the last decade, some political scientists have assumed that supranational organizations and non-state actors would take their place. In extreme form, virtual nations might emerge due to the convergence of blockchain technologies, crypto-currency, and the ability to project power and legitimacy through the virtual world. Virtual nations could be organized based on ideologies, business models, or single interests and could indeed supersede, supplement, or compete with traditional, physical nations. The army of the future should be prepared to interact and compete with virtual nations.

3. Future Capabilities and Lines of Development in Six Themes

3.1 Rethinking Phase Zero: Shaping the Human Domain

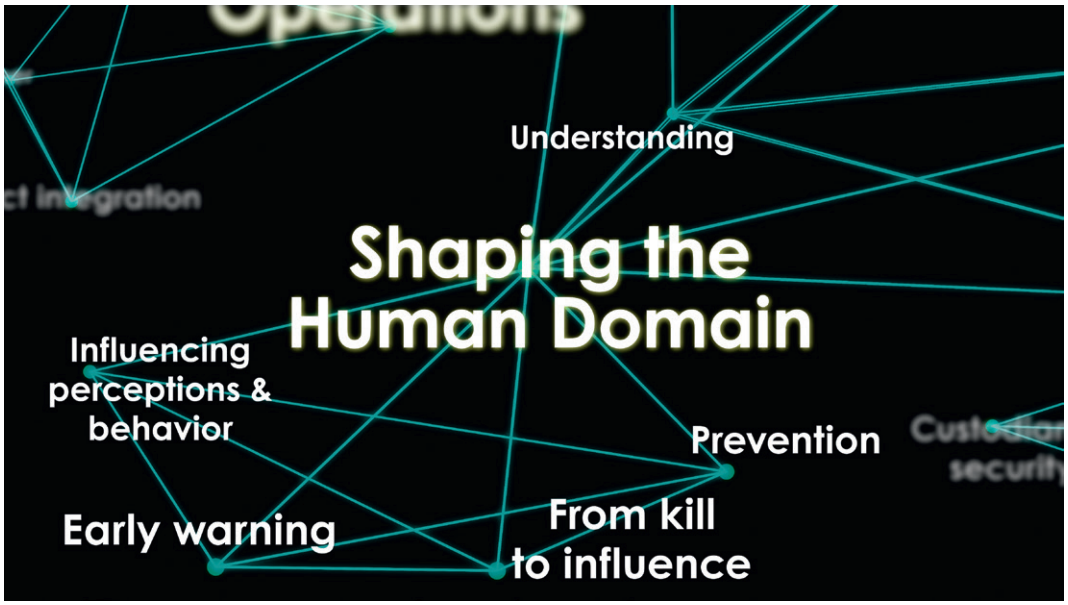

Figure 8: Shaping the Human Domain

3.1.1 What is the issue?

With the growing focus on 'war amongst the people'[38] in the past two decades and on 'influencing operations'[39] in this decade, attention has been shifting to shaping or reshaping the human domain, which can be defined as "the interaction between human actors, their activity and their broader environment".[40] Shaping the human domain requires long-term efforts, with time scopes extending beyond that of typical military operations. Largely driven by this realization, military planners have started putting more emphasis on the phase before the actual conflict starts, which some call *Phase Zero*. The initial coining of the term Phase Zero indicated the degree of discomfort military planners experienced with the interagency coordination efforts

38 Smith, *The Utility of Force*.
39 Gregg, "The Human Domain and Influence Operations in the 21st Century."
40 UK Ministry of Defence, "Understanding and Decision Making (JDP 04)." See also the second, updated version: UK Ministry of Defence, "Joint Doctrine Publication 04: Understanding and Decision-Making."

that are typical for this phase.[41] Real-life experiences, especially in Afghanistan and Iraq, gradually led to the conclusion that these not purely military shaping efforts were not unique to the early pre-intervention stages, but had to be carried out throughout the entire operation (and beyond).

As artificial intelligence becomes more advanced and starts providing us with ever more insights into the dynamics of human cognition and behavior, our ability to influence this domain is likely to increase exponentially.[42] What might become extremely relevant for trying to shape the human domain in continuous Phase Zero efforts is the way in which the knowledge and understanding about humans and their environments that lies encoded in texts and various datasets, is being decoded and structured at an exponentially accelerating pace. This is happening in academia, but even more dramatically – even if mostly under the radar screen – in a number of information behemoths such as Google, Microsoft, IBM, Amazon and Facebook, along with Baidu, Yandex, etc. One of the most intriguing aspects of, for instance, Google's Knowledge Vault, Microsoft's Concept Graph and IBM's Knowledge Graph, is that these hubs represent companies' ambitions not just to structure knowledge about their domain, but to influence human behavior in ways that are more subtle and seemingly more effective than extant ones.

Figure 9: Understanding the Human Domain in the Operational Environment

41 Which was officially removed from US doctrine in the latest version of JP-5.0 (which is now no longer called Joint Operation Planning but Joint Planning, in recognition of the blurring of the traditional 'linear' view of the 'levels' of war or echelons), although the construct of phases still remains. US Joint Chiefs of Staff, "JP 5-0, Joint Planning."

42 De Spiegeleire and Sweijs, "Artificial Intelligence and the Future of Defense."

3.1.2 Relevance for the Army: Future Capabilities and Lines of Development

Land forces (together with their Special Operations Forces colleagues) are by definition far more anchored in the human domain than their air or maritime colleagues. Civil-military capabilities tend to be embedded in our land components. These are the entities that are starting to build cumulative knowledge about the human domain in ways that may differ from our military intelligence communities, a trend which is clearly emphasized in recent work of the RNLA's Land Warfare Centre.[43] It therefore stands to reason that our land components will become the main catalysts of the shift from the kill chain to the influence chain. This would require a significant repurposing and retooling of the physical, cognitive, and digital characteristics of our current land components: from brawn to brains. And such a metamorphosis is indeed conceivable, with the following lines of capability development as examples:

Design* next to *Plan. Military planners should master the art of designing according to the human-centered tradition, next to the ability to plan in the more traditional sense.[44] Special emphasis should be on the empathy side, not merely for its own sake, but for the sake of formulating and experimenting with promising actionable options. Knowledge about the behavior, perceptions, motives, bottom lines, preferred sources of information etc. of all relevant actors, be it states, key leaders, groups, organizations or corporations, as well as their mutual relationships, is crucial. This ability can be made very concrete. Building on the experience gained with deployed Operational Analysis (OA) teams in Afghanistan, the capability to design, test and adjust campaign plan options should be strengthened. Such teams should be involved in the early design stages of potential or actual missions and could, on a case by case basis, be forward deployed in order to conduct in theatre analysis.[45]

Understand and use knowledge graphs. Military planners should become able to understand the importance of – and possibly also to build, manage and curate – knowledge graphs that include all available knowledge on the broader security issues where the Netherlands has interests and/or values at stake. This may well require that the Army intelligently and responsibly interacts with the key builders of these modern knowledge graphs (primarily Google, Microsoft, IBM and Facebook, but possibly also companies like Baidu, Yandex, and others). This requires various incentives, contractual arrangements and ethical guidelines for both sides to be designed in order to stimulate and structure these types of interactions. This can be made concrete,

43 van Dalen, Dekkers, and van Daalen, "NetForce: Een Nieuw Model Voor Toekomstige Defensie."

44 This approach maintains that 'operational plans' should be designed based on a broader *and* deeper systems-of-systems understanding of the broader security environment (in which the military-operational part is an important, but still only one part of the equation). So too should any strategic assessment also draw on the (unfettered) military-strategic experience and appreciation of our flag officers. This means that they should also be entitled to reflect upon possible future forms of strategic guidance. See De Spiegeleire, Sweijs, and Wijninga, "Designing Future Stabilization Efforts."

45 Some concrete vignettes on this are included in Bekkers et al., "Si Vis Pacem, Para Utique Pacem: Individual Empowerment, Societal Resilience and the Armed Forces."

for instance, through inwards or outwards seconded personnel in these fields – e.g. Dutch employees from these companies whose knowledge could be tapped, or Dutch military (and/or reserve) officers seconded to some of these companies.

Strengthen influence capabilities. The objective of influencing operations (stratcom, info ops, offensive psy ops, social media campaigns etc.) is to shape the situational understanding of relevant other actors, and mold their behavior. If such operations target other military actors, the responsibility (but not necessarily the execution) might lie within the armed forces' purview, as targeting a wider audience implies a whole of government (and for the execution possibly a whole of society) approach. Again, much can be potentially learned from the large knowledge companies. Training personnel in using new forms of knowledge and understanding to wield influence can be made concrete by establishing training agreements with these companies, and by giving them time and incentives to start experimenting with what they learn.[46]

3.2 Multi-Domain, Multi-Level Operations

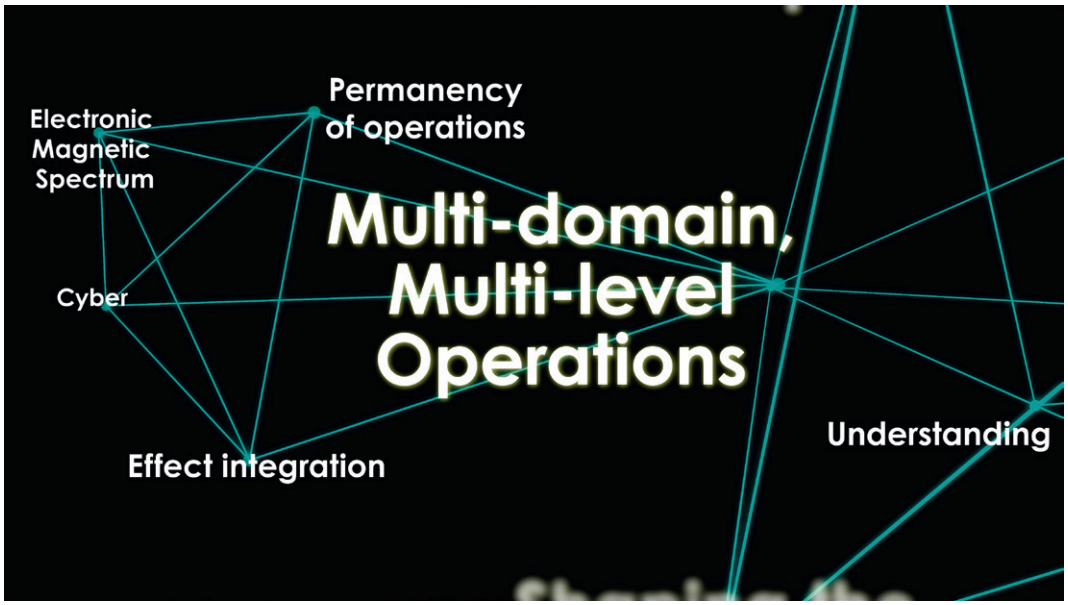

Figure 10: Multi-Domain, Multi-Level Operations

3.2.1 What is the issue?

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.

46 Because both responsibilities and execution of influencing operations extend across services, government agencies and societal actors, the training programs are ideally also conducted jointly, intergovernmentally and with non-governmental actors.

This means that to be effective, armed forces need to be able to coordinate and synchronize 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 organize to prevail in future armed conflict. Existing notions of combined arms and joint operations should be taken to the next level.

Various military organizations around the world are trying to achieve just that. The US Army Training and Doctrine Command in close coordination with the Marine Corps has formulated its vision on multi-domain battle in order to prepare the US Army for conflict in the 2025-2040 timeframe.[47] Emphasis lies on the ability to execute expeditionary maneuvers across different domains with little or no support, create 'windows of advantage' to decisively defeat the adversary in contested areas and enable other joint forces to fight and win.[48] Contemporary theatres of conflict already feature ground forces who have proven their ability to operate in a dispersed and decentralized manner for sustained periods of time, sometimes in close coordination with third actors. The Islamic Revolutionary Guards Corps operations of Iran in the Syrian theatre and beyond serves as a point in case.[49]

The morphing of the different domains of war requires much closer coordination and in some cases integration with other services. Command and support relationships will vary over time, with army units being supported at one time and delivering support at the next. For instance, when faced with advanced ISR and A2AD capabilities, the existing division of labor in which the air force weakens the opponent's military capabilities before the army moves in, may have to be supplemented with new war fighting concepts in which *ground forces* clear the way for *air forces* by puncturing A2AD bubbles.[50] The tactical-strategic level compression and the increasing tempo of operations requires tactical (land) commanders to have a better understanding of the battle space, including the multi-domain threats they face, as well as of the (superior) commander's intent at all levels in the chain of command. They also need an immediate grasp of the options, including the toolset, that they have at their disposal to swiftly address these threats.[51] It will necessitate the devolvement of discretionary decision making authority to lower ranking personnel who should be allowed to operate with greater degrees of freedom.

47 US Army TRADOC, "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040."
48 Ibid p.iii.
49 US Army TRADOC, "Threat Tactics Report: Iran." See also Alfoneh, "Iran's Revolutionary Guards Transform into an Expeditionary Force." General Suleimani heads the Iranian intervention in Syria. The expeditionary ground force under his command include 'the Afghan Fatemiyoun, Pakistani Zeynabiyoun, Lebanese Hezbollah, and the Iraqi Harakat al Nujaba.' See Toumaj, "Soleimani's Presence in Aleppo Underscores Strategy of Crushing Rebels | FDD's Long War Journal." And Alfoneh, "Iran's Revolutionary Guards Transform into an Expeditionary Force."
50 Freedberg Jr., "Miserable, Disobedient & Victorious."
51 Telley and Membrere, "Training 'No Huddle' Joint Offense."

Figure 11: Exploring the New Domains

3.2.2 Relevance for the Army: Future Capabilities and Lines of Development

The Netherlands Army is well positioned to develop a multi-domain conflict concept and the concomitant capabilities based on the four quintessential Dutch strengths. It first and foremost requires a solution oriented, multi-disciplinary approach which connects different services and agencies. The development of this approach should focus on the tactical levels of brigade and below and put the following capabilities and lines of capability development central:

The ability to integrate effects. Virtually all kinetic and non-kinetic effects brought by the various armed services (and other instruments of power) converge in the land domain. The Army should act as an effect integrator: monitor and understand the interplay between the various types of effects and their consequences, and advise on how instruments deployed by various multi-domain *effectors*, both military and non-military, should be integrated for an optimal net result.

The ability to coordinate horizontally and vertically with other actors. This is about coordinating and cooperating with different actors in a security ecosystem, working towards a common goal (unity of direction) through the use of shared standards

and systems. This includes the ability to direct Joint, Interagency, Multinational and Public (JIMP) activities and operations at the brigade level across different warfighting domains (land, sea, air, information and human domain), in close cooperation with the other services. It requires robust and reliable communications systems.

The ability of lower level commanders to exercise discretionary judgment within the general guidelines provided by the commander's intent. This underscores the importance of attention to the development of leadership skills in the training of officer-cadets and to their understanding of the interaction between tactical, operational and strategic levels of war.

The ability to sense and possibly act in the electromagnetic spectrum. This is where close cooperation with the air force is required, because many of the sensing and acting electronic warfare systems are airborne (to cover a wide area, to quickly pinpoint to certain locations or enemy assets, or both).

3.3 AI in the OODA Loop

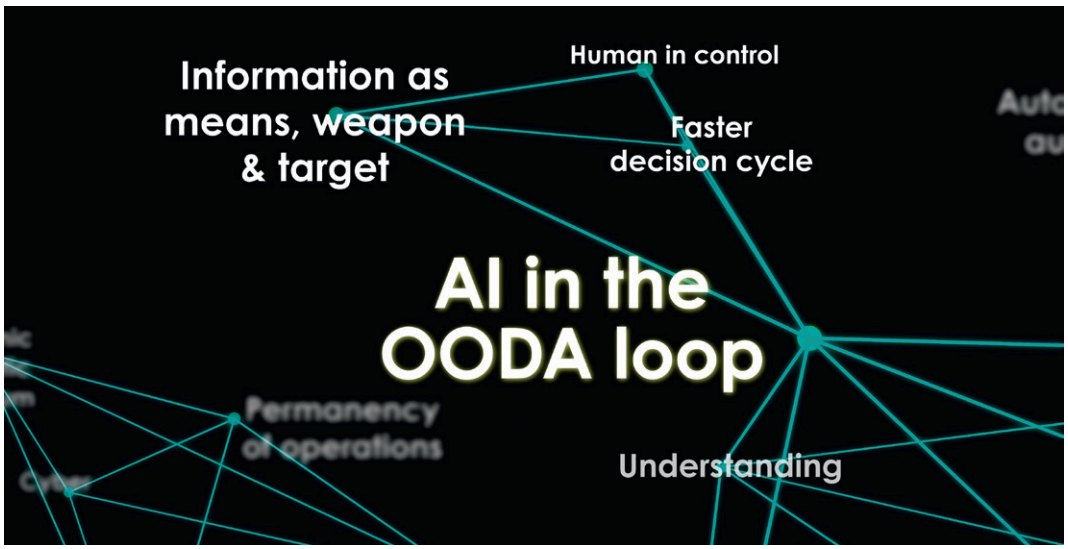

Figure 12: AI in the OODA Loop

3.3.1 What is the issue?

It is widely acknowledged that "any assessment of the likely landscape of future conflict must recognize that no matter what type of engagement, the outcome will increasingly be determined by the side better equipped and organized to gather, process, disseminate and control information."[52] Over the next decade, rapid advances in AI may create considerable capability gaps between those actors equipped with advanced AI-powered systems and those without – with unpredictable results.[53] First and foremost, superior

52 Lt Gen Deptula, "The St. Andrews Proclamation: A Pragmatic Assessment of 21st Century Airpower."
53 After Cummings et al., "Artificial Intelligence and International Affairs, Disruption Anticipated."

information will enable conflict actors to move more rapidly and thorough through the Observe-Orient-Decide-Act cycle. Furthermore, in addition to already being central in the Observe and Orient stages, and thus informing the Decide stage, information will also become the focal point in the Act stage. 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 term information-driven operations, reflecting the fact that information processed to create situational awareness and situational understanding (SA/SU) progressively shapes operations, is apt but also too limited. With information and information infrastructures becoming the center of gravity, information-*centric* operations might be the better term. In fact, the most appropriate term would be *understanding-centric* operations. Conflict is an essential human activity. It is not information as such that is the center of gravity, but how that information is interpreted and used by humans, and how that affects their behavior.

In the competition for faster and better OODA loops, the loop will increasingly become algorithmic. Big data from a combination of open sources and ambient data, non-military information providers and dedicated military sensors will capture reality to a high level of fidelity. [54] These data streams will feed directly into complex computerized models of reality (capturing many parameters and variables and interactions between them) which are not constructed by humans but developed through the use of machine learning techniques.[55] The more sophisticated models will not only generate reliable assessments of real-time situations, but will also be able to perform courses of action analysis. If at the tactical level real-time decision making is required in order to stay inside the opponent‘s OODA loop, there might not be enough time for human review of the solutions provided by the system. Automated intelligence assessments will thus spur a drive towards (semi-)automated decision-making.

In *analytical* roles, AI systems will allow humans to focus on higher-level decisions, while repetitive tasks such as monitoring sensors will be automated. The impact of those changes is likely to be attenuated rather than transformative. *Predictive* uses could have more acute impacts, though likely on a longer timeframe. Such applications may change how planners and decision makers understand the potential outcomes of specific courses of action. If, or when, such predictive AI systems become sufficiently accurate and trusted, the specter of autonomous entities fighting other autonomous entities might become reality. These developments are surrounded with a lot of strategic, ethical, legal and technical issues. The effects of some of the more transformative scenarios in this area are unlikely to materialize fully within the next decennium.

54 Ambient data is more or less readily available ‘in the environment’. For instance, smart phones already register position, temperature, speed of movement, acceleration, altitudes, humidity, and a host of other indicators.

55 In general, with many objects coming online and exchanging data in the internet of things, the idea of ‘ubiquitous intelligence’ and ‘smart objects’ is becoming reality.

Figure 13: Introducing Machine Learning in Complex Decision Cycles

3.3.2 Relevance for the Army: Future Capabilities and Lines of Development

The various OODA loops are more complex in the land domain than elsewhere. There is a lot to observe, be aware of, understand and act upon in the dense, cluttered and diverse land environment. Furthermore, land operations are inherently joint and interagency. The challenges are therefore multifaceted: how can armies achieve surprise through a superior OODA loop on an urban battlefield that is populated by a variety of threat groups and wired with cheap, connected sensors? Every civilian with a cellphone is able to collect and disseminate intelligence in real-time that opponents may be able to leverage in combination with increasingly cheap, precision fires. This implies that significantly speeding up the OODA loop at the strategic, operational and tactical levels, as well as the various feedback loops between these levels, by automating large parts of that loop, is the most challenging pursuit, but arguably also the most rewarding one, in land operations. Considering this, the following lines of capability development may be worthwhile for the Army to pursue.

Expand information base. Machine learning thrives on copious amounts of data. A prerequisite for experimentation with AI to create more comprehensive SA/SU at all levels, is allowing for wider data streams from an array of sensors and other information sources, including metadata from smartphones, drones, satellite images, special operating forces, intelligence services, internet/media analysis, anomaly detection etc.[56] (Potential) sources lie, for a substantial part, outside of the own organization. Defense has a responsibility to foster, facilitate and tap into the interagency and whole of society

56 While being aware of the security risks involved, see e.g. Vincent, "Don't Use Huawei Phones, Say Heads of FBI, CIA, and NSA." and "Global Surveillance Disclosures (2013–present)."

knowledge networks and ecosystems that are instrumental in creating strategic SA/SU – and are, to a degree, part of that creation process. Furthermore, data should be handled as it comes in. The format and mode of delivery is very much determined by the source and, in most cases, can and should not be prescribed by the recipient. A dynamic balance should be struck between tapping raw and processed data, and between face value information and interpreted knowledge.

Start introducing AI in the OODA loop. Investigate which parts of the OODA loop can best be (semi-) automated or supported using AI (machine learning) techniques. The HCSS report *Artificial Intelligence and the Future of Defense: Strategic Implications for a Small Force Provider* (2017) recommends a pragmatic attitude. The advice is to focus initially on AI applications that can be rapidly implemented in the framework of existing structures and processes (quick wins), as an agent of change for more ambitious efforts. The suggestion is to primarily reap the potential benefits of the R&D investments of the frontrunners. In particular, American, British and Israeli investments in defense AI, competing with Chinese (and possibly Russian) efforts, can be expected to be both substantial and significant. Furthermore, developing strong working relationships with the defense technological and industrial base is critical, as much of the innovation is taking place in the commercial sector. Organizing explicit feedback loops in field lab type of setups, where experiments meet operations, for evaluating and improving the analytical and predictive power of AI-based algorithms, are essential. Concrete focus areas include:

- At the strategic level: create, curate and exploit semi-automated big(gish) data models to analyze the propensity of states for (future) instability and conflict.[57] This provides the basis of an early warning system for emerging crises and conflict. Such models could well be enhanced by feeding them with near-real time data and using AI-techniques to analyze and predict outcomes. Depending on the level of granularity, fidelity and timeliness, such strategic models (or dedicated derivatives) could in the future possibly serve operational and even tactical level SA/SU as well.
- At the operational level: elements of the operational planning process, such as battlespace analysis, center of gravity analysis and courses of action development and analysis, are likely candidates to aim for experiments with AI-based (semi-) automated SA/SU creation.
- At the tactical level: in addition to focusing on artificial intelligence for autonomy, the Dutch Army should position itself to leverage commercial applications that optimize staff processes. As an example, the Army could use apps like Waze, the popular driving program, for optimizing (possibly self-driving) convoys.[58]

57 HCSS has developed a Stratbase, including a political violence risk monitor, that provides daily updated automated risk assessments of the onset of political violence worldwide on the basis of hundreds of thousands of data points.

58 Jensen and Kendall, "Waze for War."

3.4 Robotic and Autonomous Systems in the Land Domain

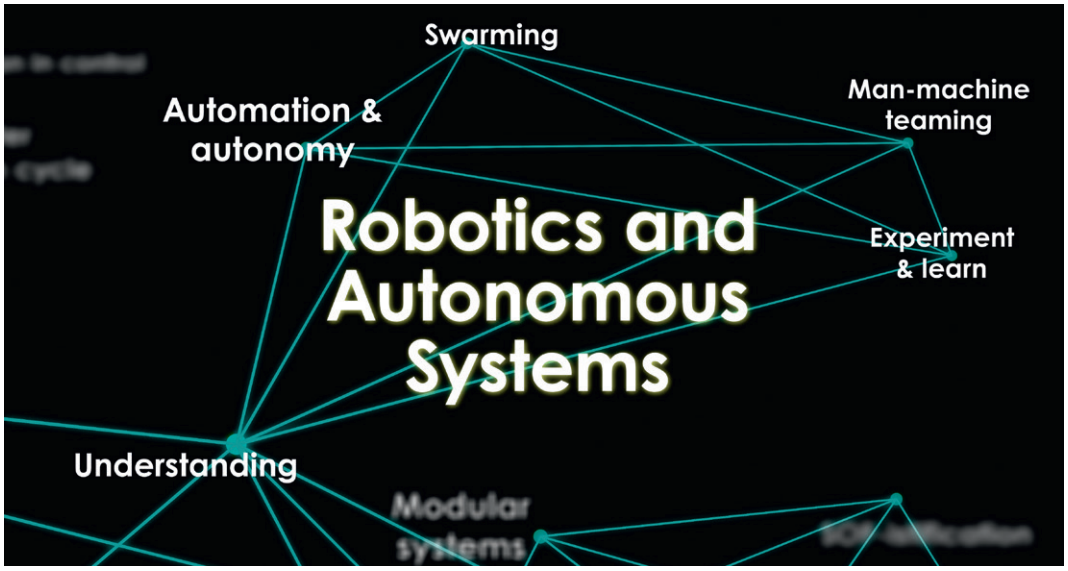

Figure 14: Robotics and Autonomous Systems

3.4.1 What is the issue?

The emergence of robotic and autonomous systems (RAS) is expected to progressively affect the face of conflict over the next decade. Rapid progress in AI propels an increasing degree of automation and autonomization of military platforms. Human operators will continue to be involved in the decision to engage targets, but along the different steps in the OODA cycle, they will increasingly be supported, and at times even be replaced, by machines.[59] Overall, RAS will significantly improve the range, persistence and mass of land forces, while being less dependent on the number of human operators that they can field.[60] Small, widely dispersed autonomous sensors contribute to increasing the situational awareness of land forces in theatre and can support targeting acquisition.[61] Through additive manufacturing, some of these auto-sensors can be produced in theatre on demand, on specs, and in real time.[62] As long as systems are not fully autonomous (which they are not expected to be for a wide range of tasks for the next decade), this will spur a 'battle over bandwidth', because bandwidth is necessary for human-machine interaction.[63]

RAS will change the economics of force acquisition (man-out-of-the-loop relaxes many design constraints), force generation (lower expenditures and possibly political

59 See Section 3.3. This section focuses on the physical side of the equation: the platforms.
60 See UK Ministry of Defence, "Human-Machine Teaming (JCN 1/18)." And Scharre, "Robotics on the Battlefield. Part I: Range, Persistence and Daring."
61 Tucker, "US Army Seeks Internet-of-Battlefield-Things, Distributed Bot Swarms."
62 Atherton, "The Marine Corps Wants to 3D Print Cheaper Drones."
63 This may also provide an incentive to some parties to cede more decision power to the machine in highly contested environments. However, bandwidth is an issue regardless of the human control issue because it is required for sensor data transmission.

constraints on deploying armed personnel) as well as force projection (higher potential safety for armed personnel). RAS will also pose a significant risk to current generation legacy platforms to become rapidly outdated. It is expected that the emergence of large numbers of disposable and miniaturized unmanned systems will render many traditional military platforms obsolete through *direct overmatch* (because of strength in numbers), and *cost ratio* (because the former will be much cheaper). Applications currently already make use of relatively unsophisticated technology available on the global market. The Army's explosive disposal unit EOD regularly employs three sizes of robot vehicles to explore and dismantle suspicious packages. The use of drones for reconnaissance and monitoring tasks is taking off too. Perhaps more nefariously, unmanned aerial vehicles carrying machine guns (which by the time of writing have already passed through the testing stage) are similarly relatively low tech.[64] Certainly more high-tech, the militaries of larger countries are experimenting with swarming concepts that rely on large numbers of unmanned systems which coordinate autonomously.[65] These are expected to be operationally ready within a decade from now.[66]

As Scharre, one of the world's leading experts on the military implications of RAS, has rightly asserted, "the winner of the robotics revolution will not be who develops this technology first or even who has the best technology, but who figures out how best to use it."[67] The battlefield of the near future may not yet be fully robotized, but is likely to be dominated by *centaur units* that effectively team up humans with machines. Human operators will be assisted by a variety of machines across a range of tasks, including logistical support, reconnaissance and intelligence, to actual war fighting, with the human operator retaining executive command over the decision to deploy force.

3.4.2 Relevance for the Army: Future Capabilities and Lines of Development

From the perspective of affordability and scalability, RAS are especially relevant to smaller and medium sized force providers such as the Netherlands. RAS first and foremost can serve as an unusual force multiplier and make up for the relatively small numbers of conventional platforms that the Netherlands can field. What is more, both the software applications and the operational concepts underlying the effective use of RAS tend to be scalable. Finally, also from a political and economic cost perspective, the integration of smaller RAS is appealing.

---

64 Dormehl, "Meet TIKAD."
65 For China, see Kania, "Swarms at War." For the US, see "Service Academies Swarm Challenge Pushes the Boundaries of Autonomous Swarm Capabilities." Note that it is not so much the swarm elements that are high-tech, but the algorithms (which have not been quite mastered) that drive effective swarm behavior.
66 National Academies of Sciences, Engineering and Medicine, "Discussion of Selected Topics from the Restricted Report."
67 Scharre, "Robotics on the Battlefield. Part I: Range, Persistence and Daring," 9.

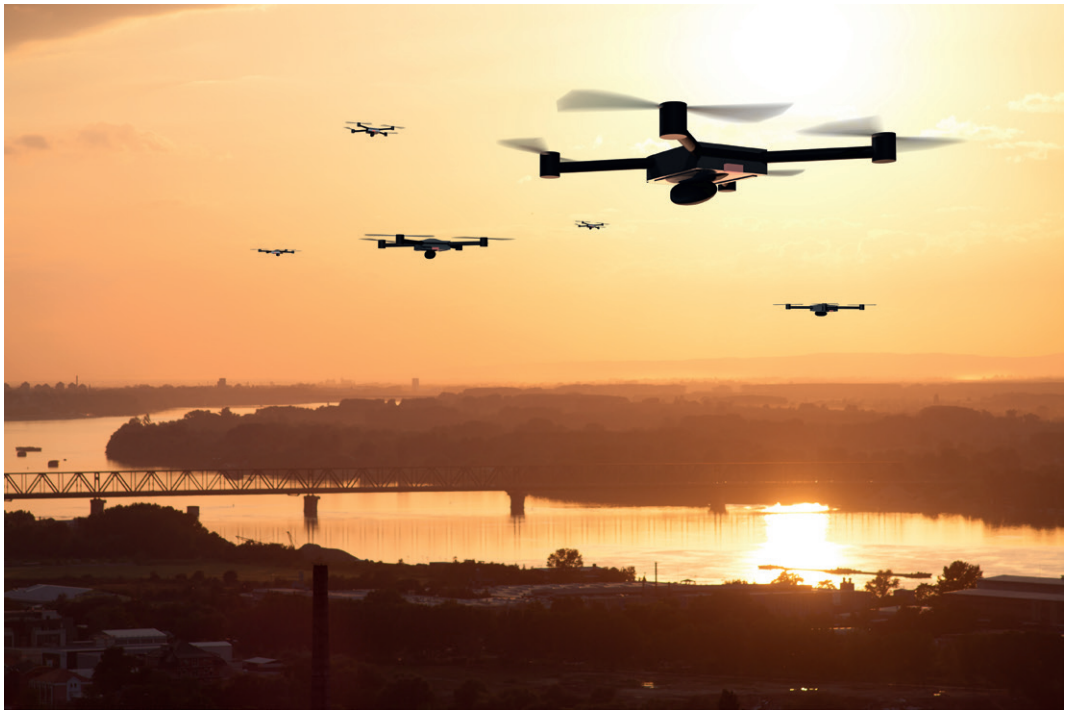

Figure 15: The Robotized Battlefield

The Dutch Army is well positioned to experiment with RAS technologies. It has recently set up the first small-scale RAS unit which will be allowed to grow organically over the next few years. New configurations for human-machine teaming should be experimented with in training settings, using off the shelf technology. Experimentation and learning are the key terms here. Short and rapid prototyping loops should facilitate the speedy translation and implementation in operational concepts and doctrine for land forces. Partnerships with the research and development community should be actively pursued. The Delft University of Technology, one of the world's leading technical universities, is home to the Robotics Institute and RoboValley, an initiative to foster close collaboration with industry.[68] For now, the Army's RAS unit should not focus on the development or acquisition of major unmanned land platforms. Instead, it should prioritize creating relationships with developers and producers of the relevant technologies, and building knowledge and experience (through concept development & experimentation) about how to effectively employ RAS. Against this background, the Dutch Army should focus first and foremost on the future integration of unmanned land-based and airborne systems in land operations. The following lines of capability development merit further exploration:

Focus initially on RAS in combat support and combat service support. The use of weaponized autonomous systems poses a host of ethical and legal questions and

68 Arthur de Crook, "Interactive Robots, Robots That Work and Swarm Robots," TU Delft Robotics Institute, accessed July 2, 2018, https://tudelftroboticsinstitute.nl/research; "RoboValley."

dilemmas, next to operational challenges. In order for the Army and its stakeholders to get accustomed to the use of robots in the military, it is advisable to start with support rather than combat systems. Many sensor, logistics, transport etc. systems lend themselves for full automation.[69] At the same time, it is inevitable that shooter systems will also become more autonomous, starting with defensive systems for e.g. missile defense and compound protection.

Centaur units. Start experimenting with *centaur units* that leverage the strength of machines to reduce the exposure of Army personnel to enemy fire (think of the so-called *wall of robots*) *and* create mass while reducing the number of boots on the ground. Concrete areas to initially focus on are:

- Small sensor systems which can be flexibly deployed by combat teams in theatre for more dedicated real time situational awareness. An example is the use of small airborne autonomous sensor systems to survey and monitor the surroundings,[70] or the situation inside buildings.[71]
- Autonomous electronic warfare systems that help in gaining dominance in the electromagnetic spectrum. This is essential in an environment where being (and staying) connected is a crucial condition for success. Such systems may also provide counter-A2AD capacity, mislead opponents through the saturation of sensors, and provide defense against enemy UAVs.
- Semi-autonomous land-based and/or airborne logistical support systems, which will enable the Army to conduct land operations with a significantly reduced footprint.

Create conditions for rapid scaling and expansion of RAS applications by monitoring technological developments and Concept Development & Experimentation (CD&E) projects by partner countries and by building a national and international knowledge network with industry and knowledge institutes. In a decade from now platforms such as the armored personnel carrier CV90 35NL, the artillery howitzer PzH2000NL, the multi-role armored vehicle Boxer and the reconnaissance vehicle Fennek are due for replacement. To make informed decisions about which functionalities could be best covered using RAS (and which not), the knowledge and experience gained through these CD&E initiatives are essential.

69 And may contribute to reducing the footprint of military deployments, thereby reducing vulnerabilities, cost and environmental impact.
70 See Eshel, "Soldier Borne Sensors | Defense Update."
71 Ureña, Hernández Alonso, and García Domínguez, "Sensors and Sensing in Indoor Localization, Tracking, Navigation and Activity Monitoring."

3.5 Mosaic Warfare: Distributed and Networked Capabilities

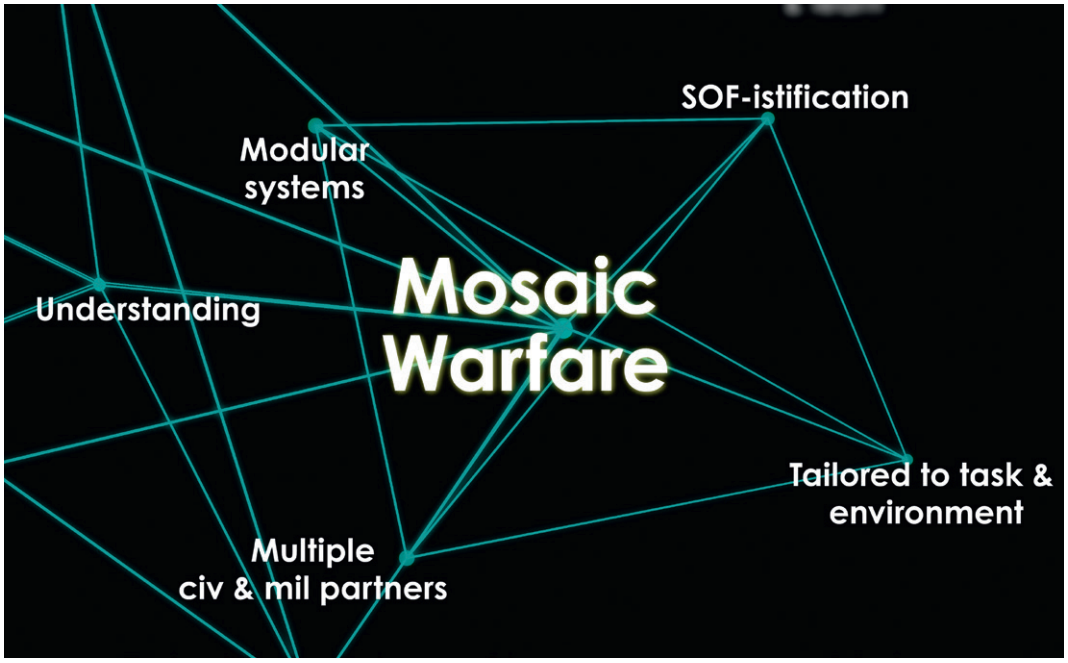

Figure 16: Distributed and Networked Capabilities

3.5.1 What is the issue?

The operating environment is characterized by competition and conflict in and across *multiple domains*; by operations conducted with *multiple partners*; and by the need to offer and pursue *multiple options* in dealing with evolving conflict situations. In the face of complex and highly dynamic threats and challenges, adaptiveness is arguably *the* defining feature of effective armed forces. On top of this, the pace of innovation has accelerated. The traditional defense development and procurement model, which is centered around intricate and expensive platforms and systems that are obtained in a semi-closed defense-specific market and that remain, largely as-is, in the inventory for decades, is unfit to reap the benefits of emerging technologies, which are largely developed in global innovation networks.

An alternative approach is to focus on smaller, dedicated and relatively cheap 'units of action' that can intrinsically scale and upgrade quickly and easily. By creating a dynamic 'mosaic' of such units (unmanned systems, small teams or combinations) that operate both autonomously and in coordination, massive complexity can be imposed upon adversaries, thereby creating strategic advantage via asymmetric means. The above concept is intended to revolutionize the innovation time cycles and adaptability of military capabilities. The engineering burden moves from the tight integration of a unit or a platform and key subsystems to the connectivity and command & control of an entire battle network. The value shifts from the performance characteristics of individual platforms to the resilience of a

heterogeneous collective.[72] Critical to this approach is a bottom-up composition ability, which can combine individual elements to create the desired overall effect, often in ways not previously contemplated. Furthermore, the notion of 'full development' is almost obviated because the distributed approach enables enduring, rapid and open-ended adaptability.

This approach starts with unravelling military functions in such a way that capabilities can be built in a modular manner. Modularity, "building a complex product or process from smaller subsystems that can be designed independently yet function together as a whole", in itself is nothing new.[73] In fact, within the military domain, it has become fashionable to think in 'building blocks' that are part of a 'toolbox' which, as a whole, offers the flexibility to confront a range of challenges through recombining modules into tailor-made configurations. The concept applies both to the level of systems (e.g. the Boxer multirole armored fighting vehicle with its reconfigurable mission modules) and of units (task forces compiled for the mission at hand). In that sense, mosaic warfare is the next – but major – step down a path that has already been taken. A crucial design principle that must move to the next level is *loose coupling,* minimizing the dependencies between modules, making the (technical and functional) interfaces and modules as simple and as self-contained as possible.[74] This allows for the quick assembly of various operational solutions from different combinations of modules. Current modular systems and units are mostly tightly coupled, resembling more of a puzzle with specifically shaped pieces fitting together in a unique way, rather than a mosaic with easy replaceable tiles.[75]

Although the mosaic warfare concept is often associated with unmanned systems that act together in swarms, this is certainly not the sole incarnation. Certainly in the land domain, soldiers are indispensable nodes in a distributed network, because they have the all-round cognitive skills to act autonomously in an adaptive way (if so trained and tasked).[76] This, in fact, accurately describes the way modern Special Operations Forces (SOF) operate: "SOF often conduct distributed operations with small operational and logistics footprints far from major bases. SOF employ sophisticated communications

---

72 A key vulnerability, therefore, is the reliance on resilient and secure communications. Robust networks that gracefully degrade and have self-organizing and self-healing qualities are a prerequisite for distributed and networked capabilities and operations.

73 Baldwin and Clark, "Managing in an Age of Modularity."

74 Loose coupling is evident when elements affect each other "suddenly (rather than continuously), occasionally (rather than constantly), negligibly (rather than significantly), indirectly (rather than directly), and eventually (rather than immediately)" (Weick, "Management of Organizational Change among Loosely Coupled Elements.")

75 For example, the interface between the two key modules of the Boxer multirole armored fighting vehicle, the platform / drive-line and the removable mission module, is very specific (and proprietary). There is still a huge premium on designing the modules that need to be integrated in concert so as to guarantee interoperability.

76 The effect of technologies on land are often not as great as in other domains due to geography, the interaction with adaptive enemies, the presence of non-combatants, and other complexities of the land (and human) domain. The soldier, as the core of a soldier-'system', remains central for the army. "Recent and ongoing conflicts reinforce the need to balance the technological focus of army modernization with a recognition of the limits of technology and an emphasis on the human, cultural, and political continuities of armed conflict." From US Army TRADOC, "The U.S. Army Operating Concept 2020-2040."

systems [...]".[77] As the USSOCOM mission statement reads: "USSOCOM [...] provides Special Operations Forces to support *persistent, networked and distributed [...] operation*s in order to protect and advance our Nation's interests".[78]

3.5.2 Relevance for the Army: Future Capabilities and Lines of Development

We envision the following lines of capability development:

Further the 'SOF-istication' of the Army. Even if in some aspects the Cold War seems to have returned – with interstate conflict, once again, a realistic option to plan for – this does not herald the return to large mechanized formations. Western technological superiority has eroded and potential adversaries have access to effective A2AD-capabilities. To be able to operate in A2AD-bubbles, dispersion, concealment and (up to a point) intermingling with civilian populations is required. Stealth and mobility is key. This tendency is reinforced by the fact that future operations will increasingly take place in build-up areas. Operating in urban environments typically requires decentralized combined arms as well as joint capabilities.

In recent years, we have seen the emergence of 'SOF-capable' units that fill the gap between regular and SOF units.[79] In light of above observations, this line of development advocates for the continuation of this trend: a number of the current characteristics of SOF-units and SOF-operations should be structurally applied to larger parts of the regular Army. Among these characteristics are the ability (or even the appetite) to maneuver in small(er) combined arms teams; to operate and fight 'amongst the people' with high levels of cultural awareness so as to exploit the human domain; to routinely operate with other partners at all levels; to develop an understanding of complex situations in depth, breadth, and context through the integration of intelligence and operations; to tease, test, and probe as to create one's own opportunities and do not operate on others' timelines; all whilst retaining the Army's critical ability (typically lacking for SOF-units proper) to create mass. Even when operating dispersed, mobile combined arms teams must be able to concentrate their efforts rapidly to, for example, isolate the enemy or to attack critical enemy assets. Since SOF-units tend to have more advanced and up-to-date equipment and more rigorous and continuous training

77 US Joint Chiefs of Staff, "JP 3-05, Special Operations."
78 See https://www.socom.mil/about; our italics. Note that the elements persistent, distributed and networked apply to all levels. At the strategic level, for instance, unity and continuity of effort is not so much a matter of having real-time communication links to coordinate actions, but can be achieved through e.g. staggered SOF unit rotations. Also, at that level, the networks are not tactical networks deployed by the SOF units themselves, but rather interagency networks and social networks with key host nation personnel.
79 See Bekkers, De Spiegeleire, and Wijninga, "Special Operations Forces: Schaduwkrijgers in Het Licht van de Toekomst."

programs, this line of development would require that the quality norms for regular army soldier systems in terms of equipment and training are adjusted upwards accordingly.[80]

Figure 17: Connected with Distributed Non-military Assets

Make use of distributed and connected non-military assets. One of the underlying principles in this and other themes is the cooperation with other agencies and societal groups in support of military tasks and missions. Cooperation with volunteers through social media and web applications to perform complex pattern analysis in disaster relief and crisis situations is an already standing practice.[81] Such initiatives should be expanded and strengthened. In addition to exploiting existing infrastructure, networks could also be created on an ad-hoc basis. Why not distribute cell phones to locals in a mission area and let them take photos of the situation on the ground that are then automatically geotagged and uploaded to a military intelligence network?[82] The line of development would be to enhance the civil-military interaction capabilities to liaise with local parties in order to make them implicitly or explicitly part of a distributed intelligence network that enhances (military) SA/SU.

Extend reach with (semi-)autonomous capabilities. By equipping soldiers and small teams with (semi-) autonomous operational capabilities, the soldiers' reach

80 We do not imply that the regular army is replaced by SOF. Indeed, by definition the regular army cannot be special. But this line of development underlines a tendency that some of the 'special' features that make SOF-units so effective become adopted by the army at large. These features then become the 'new normal', while SOF-units move on to ever more advanced competencies and tools.

81 See Nhan, Huey, and Broll, "Digilantism."

82 In the conflict with Ukraine, Russia has allegedly distributed cell phones among sympathizers with the request to take photographs of UKR military vehicles. These phones automatically ensured that after taking a picture it was sent to Russian intelligence, including geographical coordinates. Target verification was then done with drones before artillery fire was issued (classified source).

can be extended in order to improve situational awareness, create better protection and possibly increase lethality. Integrated man-machine teaming arrangements in challenging (combat) operations requires unconditional, mutual trust, which takes time to build.[83] A growth path is feasible and already underway (see Section 3.4). The level of autonomy granted to distributed systems – not only for stand-alone tasks, but as an integral part of complex missions – increases over time as confidence builds and the operational experience gained improves the decision making logic of the systems. The focus in this line of development should not be on the technology itself, which can typically be obtained on the market, but on the exploration of new possibilities and limitations (made possible by emerging applied technology); trust building; and on doctrine and tactics development.

Experiment with swarming. The next step would be to exclude the human from the operational loop and put them into a supervision role. As Scharre notes, "Collectively, swarms of robotic systems have the potential for even more dramatic, disruptive change to military operations. Swarms of robotic systems can bring greater mass, coordination, intelligence and speed to the battlefield, enhancing the ability of warfighters to gain a decisive advantage over their adversaries."[84] A significantly larger number of much cheaper systems, purpose-built for specific missions, complicates the targeting objectives of adversaries and allows for the graceful degradation of combat power as assets are destroyed. It also allows a family-of-systems approach, increasing diversity and reducing technology risk, which again drives down costs. The power of coordinated, intelligent and fast action swarming lies not just in greater numbers. Swarming also enables synchronized mass attack and defense, more efficient allocation of assets over an area, self-healing networks that respond to enemy actions, and widely distributed assets that cooperate for sensing, deception and attack. Harnessing the power of swarming will require new command-and-control models for human supervision beyond existing paradigms where humans directly control a vehicle's movements. Again, many of the underlying technologies behind increased autonomy are driven by commercial sector innovation, and as a result, will be available to a wide range of state and non-state actors. It is therefore high time to start experimenting and innovating together with close partners in triple helix arrangements.[85]

Apply a distributed and networked approach to peacetime functions. The mosaic paradigm is not just an operational challenge. It requires, in some instances radically, different structures and processes for development, acquisition, lifecycle management (MRO), recruitment, training and readiness. In fact, an experimental mindset may be as

83 See the innovation target *Human-machine teaming* in Ministerie van Defensie, "Strategische Kennis- en Innovatieagenda 2016-2020: Voorblijven in een onveiliger wereld.". 40-41.
84 Scharre, "Robotics on the Battlefield Part II," 5.
85 Triple helix cooperation in our context points at new forms of public-private partnerships where defence organisations (and government agencies in general) closely cooperate with industry and knowledge institutes aimed at innovation trajectories that offer real added value for the end user.

much required to innovate the relevant administrative organization, rules and procedures as it is for operational capabilities and doctrine. Some illustrative examples are:

- Stimulate the secondment of officers, as part of their career, with partners in the national and international security ecosystems, defense and security think tanks, businesses (not just the usual suspects, but with the big tech companies, innovative startups etc.).
- Create triple helix cooperation frameworks for continuous concept development & experimentation and technology insertion.
- Create distributed training facilities. Much can be learned from the way online distributed games work.

3.6 Empowering the Agents of Resilience

Figure 18: Empowering the Agents of Resilience

3.6.1 What is the issue?

Most military planning and thinking tends to focus on the acute phase of the contest of wills, in which opponents confront each other across a battlespace. That phase is characterized by enormous difficulties and has led to many painful experiences in military engagements over the past two decades. As a result, political and military leaders are putting more emphasis on prevention and resilience. This section deals with the latter (with the former covered as part of the discussion in Section 3.1).

Even in cross-domain (hybrid) battlespaces and despite the rise of autonomous systems, humans will continue to play an important physical and cognitive role in managing the human dimension of almost all security situations for at least the foreseeable future. As we have argued before, the land component of our armed forces

is the most human-centric one in the sense that land forces often operate in the middle of highly dense societies. By that token, land forces are in the best position to identify and track the healthy fibers of a society, and assess which capabilities could empower those secure healthy fibers against the agents of conflict. In fact, the realm of *resilience* may very well prove to be a uniquely attractive market for highly effective capability investments by our land components. It is also a market with investment opportunities that might prove to be both more affordable and palatable to our post-modern societies compared to more kinetic options.

Opportunities in this realm are abound. Despite all of the worrisome developments in the world, this still remains a golden age of global personal empowerment. HCSS has been reporting regularly on developments in this area.[86] Technological breakthroughs in (renewable) energy, water purification and irrigation, health, education, mobility, finance etc. are dramatically increasing the likelihood that the very conditions that have historically led to socio-political confrontations and conflict can now be flipped around to create thriving communities and markets that focus their energy on productive endeavors.[87] This creates unprecedented opportunities for defense and security professionals to monitor these developments through a security lens, while remaining vigilant of how some of these trends could be stimulated to bolster security resilience.

Building or supporting resilience is not only a matter of the better known 'psychological operations' or of 'winning the hearts and minds' efforts – two human-centric aspects of the more Manichean 'us' versus 'them' realm of the agents of conflict. If we take the example of AI, for instance, smart algorithms that can more quickly detect 'red' propaganda and counter it with more effective 'blue' propaganda still belong to the conflict realm. In contrast, smart algorithms that could more quickly detect any form of ('red' or 'blue' or any other color) fake news and could then either filter it out beforehand or accompany it with more trustworthy genuine facts and/or a more balanced interpretation of these facts would belong to the resilience realm.[88]

If we look a bit further into the future, technology is on the cusp of being able to decode the knowledge that humans have been encoding in language for centuries through breakneck speed developments in natural language understanding (see Section 3.1). Combined with the proliferation of networked sensors (for civilian

86 Latest edition: De Spiegeleire, Sweijs, and Bekkers, "Strategische Monitor: Stilte Voor de Storm?"; Bekkers et al., "Si Vis Pacem, Para Utique Pacem: Individual Empowerment, Societal Resilience and the Armed Forces."

87 Only in the last 3 years, a half a billion people gained access to financial services. The Economist, "Special Report: Financial Inclusion Is Making Great Strides."

88 De Spiegeleire and Sweijs, "The Rise of Populist Sovereignism: What It Is, Where It Comes from and What It Means for International Security and Defense"; Jans and Sweijs, "Monthly Alert: Vital European and Dutch Security Interests | HCSS."

purposes), this should lead to an unprecedented ability to track and understand the human dynamics that lead to either strengthened or weakened societal resilience.

Figure 19: The Army as Facilitator in Empowering the Agents of Societal Resilience

It is clear that prevention and resilience building is predominantly civilian in nature; that a lot of government actors, civil society, NGOs and possibly IOs may have a stake; and that the military, if any, have a supportive role. But at the same time it is increasingly being realized that security is fundamental for economic and societal progress, and that armed forces have unique core competencies in enhancing security. Furthermore, military organizations are well organized and by that token can generate (some) order and structure for others to operate in and by, even if their role as operators is quite limited. This is not meant in a hierarchical sense of taking command and telling others what to do, but instead taking on a facilitating role. This manifests by way of acting as adviser, standard setter, facilitator, supervisor, or de-facto regulatory power in environments where no single actor has the incentive or the mandate to do so. This shift requires adjustment of the traditional military mindset.

3.6.2 Relevance for the Army: Future Capabilities and Lines of Development

Land forces as the custodian of the human domain. In the effort of building societal resilience against security threats, the RNLA could take the role of custodian of the human terrain (see the lens of that title in Section 2.3.3). This does not only apply to missions in foreign countries but also nationally. Here are some concrete future capability investment options:

- The ability to responsibly track (in near-real time) drivers of security resilience from the macro- (e.g. country) to the micro-level (e.g. the individual) through

automated and anonymized data exchanges with public and (especially private) data collectors.

- The ability to assess which ongoing Dutch non-defense-related (diplomatic, economic, development, investment, etc.) public *and* private efforts offer the greatest promise of security resilience enhancements and how the Dutch defense organization might be able to tweak those from a defense and security point of view.
- The ability to identify and monitor key (individual or group) agents of resilience and to increase their centrality in that system.
- The ability to engage intelligently and responsibly with social media and other internet platforms to explore how they can start playing a more positive role in strengthening or at least sustaining security resilience.
- The ability to design promising sustainable security solutions in fragile areas where new drivers of resilience are eroding or emerging.

4. Findings and Concluding Remarks

The character of contemporary conflict is changing. Recent conflict theatres have featured a series of military-strategic innovations in a process that is expected to continue unabated in the years to come. Armed forces need to adapt accordingly. Small and medium sized force providers are well advised to play to their strengths in adapting to these new challenges, not in the least because *techflation* has led to a significant decrease in the number of platforms that they will be able to field. In this context, the RNLA has asked HCSS to identify promising new or to be renewed capabilities, to inform its ongoing transformation efforts. These efforts are likely to receive additional momentum in the Defense Review of 2020. Relying on a multimethod approach, the research project team has approached new capabilities both from the demand side (the type of challenges the RNLA will be presented with) and the supply side (what type of solutions can be envisaged to deal with these challenges). In addition to relying on future conflict scenarios to explore both the threat and the solution space, the project team leveraged key strengths of the Netherlands and alternative perspectives on the role of armed forces to generate six future oriented themes that point to promising and typically unexplored or underexplored capabilities or lines of capability development that the RNLA can pursue.

Table 3 summarizes the key findings of our study. The themes *Multi-domain, Multi-Level Operations* and *Empowering the Agents of Resilience* largely fit within the current notion of the RNLA and point to capabilities that require an intensification and expansion of ongoing efforts rather than to radically new capabilities. Other themes build on developments that have already been set in motion but that are still in their very early days, such as *AI in the OODA Loop* and *Robotic and Autonomous Systems*. Exploring and building the capabilities that arise in the context of these themes will need significant experimentation with moving targets because these capabilities are under rapid development. The capabilities raised within the *Rethinking Phase Zero* and *Mosaic Warfare* themes will require considerable expansion of the existing mindset and prevailing practices. The development of these capabilities will necessitate entrepreneurship to get them off the ground and senior level commitment to see them materialized.

It is crucial that the rate of innovation within the Dutch armed forces accelerates, and that the capacity for initiating and guiding these innovation processes is strengthened.

This should be done in recognition of the fact that the bulk of innovation stems from the civil sector and that many technological developments – certainly those at the crossroads where complementary technologies meet – are exponential. This requires other forms of civil-military cooperation and a procurement strategy that enables continuous innovation. To get things moving, the armed forces should redesign innovation processes and adjust bureaucratic structures by:

- **Scaling from the edge**, by setting up workshops to freely experiment with technology areas that are developing rapidly. In these workshops, suppliers, researchers, developers and end users have room to jointly develop and experiment with new products and concepts. These will serve as test beds for innovations with immediate feedback loops to and from practitioners on the ground.
- **Stimulating adaptation and renewal as a continuous process**. The armed forces need a multi-speed acquisition process with different innovation cycles for platforms and for the systems on those platforms. Platforms (ships, aircraft, vehicles) typically take many years to acquire and have a twenty year plus lifespan. On-board systems (ICT, sensors, shooters) currently run on a similar cycle, which means that they are often outdated even before their first commissioning. This regime has to be replaced with an incremental, plug-and-play approach in which systems are modernized in a modular fashion.
- **Linking innovation to anticipation.** The armed forces need to institutionalize a permanent technology watch and assessment function which conducts long-term horizon scanning of emerging technologies with a potentially disruptive impact, and monitors new military-relevant products and services that come on the market. The latter becomes more important because armed forces seek to become smart integrators that increasingly leverage commercial civil technologies. Technology watch and assessment should be conducted in close association with a general anticipation function that assesses trends, developments, threats and opportunities in the global security environment.

These adaptations of existing processes and structures will greatly enhance the ability of the armed forces to pursue promising new capabilities across the six themes, as summarized in Table 3 on page 53. This, in turn, will enable the RNLA to continue making important contributions to national and international security for the next decade and beyond.

Theme	What is the issue?	New/renewed capabilities and lines of development
Rethinking Phase Zero: Shaping the Human Domain	In the context of wars amongst the people, shaping or reshaping the human domain has gained in importance. These efforts continue throughout the conflict curve, requiring long-term efforts with time scopes beyond that of typical military missions. In the actual conflict phase, land forces will become important catalysts for the shift from the *kill chain* to the *influence chain*. Our ability to influence the human domain is likely to increase exponentially.	• *Design* next to *plan* • Understand and use knowledge graphs • Strengthen influence capabilities • Strengthen (forward deployed) capability to design campaign plans
Multi-Domain, Multi-Level Operations	The tactical-strategic level compression, an increased operational tempo and the simultaneous conduct of operations across the land, air, sea, space, information and human domains require that existing notions of combined arms and joint operations should be taken to the next level. Commanders at all levels in the chain-of-command must have a better understanding of the battle space, including the multi-domain threats they face, and of the instruments and options to address these threats.	• Integrate multi-domain effects • Coordinate horizontally and vertically with other actors • Strengthen lower level commanders' ability to exercise discretionary judgment • Sense and act in the electromagnetic spectrum
AI in the OODA Loop	The outcome of all forms of future conflict will increasingly be determined by the ability to gather, process, disseminate and control information, and use that information to create superior situational awareness and situational understanding. In the competition for faster and better OODA loops, advanced AI-powered systems will increasingly affect the loop, especially in the land domain.	• Expand information base • Introduce AI in the OODA loop • Create, curate and exploit big (sizable) data models • Experiment with AI for center of gravity analysis, battlespace analysis and courses of action development • Leverage commercial applications for optimization
Robotic and Autonomous Systems (RAS)	RAS are expected to progressively affect the face of conflict. Over the next decade, the battlefield will likely see the advent of *centaur units* that effectively team up humans with machines. RAS will pose a significant risk to current generation platforms, as they might become rapidly outdated. Because of their (relative) affordability and scalability, RAS are especially relevant to smaller and medium sized force providers.	• Invest in semi-autonomous logistical support systems • Experiment with human-machine teaming to reduce personnel risk • Deploy small sensoring systems • Build up autonomous electronic warfare capabilities • Create conditions for rapid scaling and expansion
Mosaic Warfare: Distributed and Networked Capabilities	The concept of mosaic warfare takes the next step in modular capabilities with small, dedicated and cheap units-of-action that can intrinsically scale and upgrade quickly and easily. This requires loose coupling, with the technical and functional interfaces between modules as simple, and the modules as self-contained, as possible. Modular units must be able to operate in and across multiple domains, with multiple partners, and to offer and pursue multiple options in dealing with evolving conflict situations.	• Further the 'SOF-istication' of the Army • Use distributed and connected non-military assets • Extend reach with (semi-)autonomous capabilities • Develop swarming techniques and concepts • Apply the mosaic approach to peacetime functions
Empowering the Agents of Resilience	Technological breakthroughs create unprecedented opportunities to track and understand the human dynamics that strengthen or weaken societal resilience. Human-centric land forces are in the best position to identify and track the healthy fibers of a society and assess which capabilities could empower and secure those healthy fibers against the agents of conflict. Building resilience is predominantly civilian in nature, but the realm of resilience may very well prove to be a uniquely attractive market for effective capability investments by land forces.	• Track drivers of security resilience in real-time • Assess non-defense-related public and private efforts • Identify and monitor key agents of resilience • Engage with and explore roles of media platforms • Design promising sustainable security solutions in fragile areas

Table 3: Six themes leading to new or renewed Army capabilities and lines of development

5. Bibliography

Alfoneh, Ali. "Iran's Revolutionary Guards Transform into an Expeditionary Force." Atlantic Council, April 4, 2017. http://www.atlanticcouncil.org/blogs/menasource/iran-s-revolutionary-guards-transform-into-an-expeditionary-force.

Arms Control Association. "Worldwide Ballistic Missile Inventories," December 2017. https://www.armscontrol.org/factsheets/missiles.

Atherton, Kelsey D. "The Marine Corps Wants to 3D Print Cheaper Drones." Popular Science, September 13, 2017. https://www.popsci.com/marine-corps-3d-printed-drones.

Baldwin, Carliss Y., and Kim B. Clark. "Managing in an Age of Modularity." *Harvard Business Review*, no. September-October 1997 (September 1, 1997). https://hbr.org/1997/09/managing-in-an-age-of-modularity.

Bekkers, Frank, Stephan De Spiegeleire, Tim Sweijs, and Willem Oosterveld. "Si Vis Pacem, Para Utique Pacem: Individual Empowerment, Societal Resilience and the Armed Forces." The Hague Centre for Strategic Studies, December 17, 2015. https://hcss.nl/report/si-vis-pacem-para-utique-pacem-individual-empowerment-societal-resilience-and-armed-forces.

Bekkers, Frank, Stephan De Spiegeleire, and Peter Wijninga. "Special Operations Forces: Schaduwkrijgers in Het Licht van de Toekomst," July 9, 2015. https://hcss.nl/report/special-operations-forces-schaduwkrijgers-het-licht-van-de-toekomst.

Bendett, Samuel. "Red Robots Rising: Behind the Rapid Development of Russian Unmanned Military Systems." The Strategy Bridge, December 12, 2017. https://thestrategybridge.org/the-bridge/2017/12/12/red-robots-rising-behind-the-rapid-development-of-russian-unmanned-military-systems.

Bergen, Peter, David Sterman, Alyssa Sims, Albert Ford, and Christopher Mellon. "World of Drones, Examining the Proliferation, Development, and Use of Armed Drones." International Security In-Depth Report. Washington, D.C.: New America, March 15, 2017. https://www.newamerica.org/in-depth/world-of-drones/.

Crook, Arthur de. "Interactive Robots, Robots That Work and Swarm Robots." TU Delft Robotics Institute. Accessed July 2, 2018. https://tudelftroboticsinstitute.nl/research.

Cummings, M. L., Heather M. Roff, Kenneth Cukier, Jacob Parakilas, and Hannah Bryce. "Artificial Intelligence and International Affairs, Disruption Anticipated." Chatham House Report. London: Chatham House, June 2018.

Dalen, J.A. van, P.A.P. Dekkers, and A.F. van Daalen. "NetForce: Een Nieuw Model Voor Toekomstige Defensie." *Militaire Spectator*, March 2017. https://www.militairespectator.nl/sites/default/files/teksten/bestanden/Militaire%20Spectator%203-2017%20Dekkers%20Netforce.pdf.

Davis, Paul K. "Lessons from RAND's Work on Planning Under Uncertainty for National Security," 2012. https://www.rand.org/pubs/technical_reports/TR1249.html.

De Spiegeleire, Stephan, and Tim Sweijs. "Artificial Intelligence and the Future of Defense." The Hague, the Netherlands: The Hague Centre for Strategic Studies, May 17, 2017. https://hcss.nl/report/artificial-intelligence-and-future-defense.

———. "The Rise of Populist Sovereignism: What It Is, Where It Comes from and What It Means for International Security and Defense." The Hague Centre for Strategic Studies, September 14, 2017. https://hcss.nl/report/rise-populist-sovereignism-what-it-where-it-comes-and-what-it-means-international-security.

———. “Volatility and Friction in the Age of Disintermediation: HCSS StratMon 2016-2017 Annual Report.” The Hague Centre for Strategic Studies, 2017.

De Spiegeleire, Stephan, Tim Sweijs, and Frank Bekkers. “Strategische Monitor: Stilte Voor de Storm?” The Hague Centre for Strategic Studies, April 13, 2018. https://hcss.nl/sites/default/files/files/reports/180329%20Strategische%20Monitor-web.pdf.

De Spiegeleire, Stephan, Tim Sweijs, and Peter Wijninga. “Designing Future Stabilization Efforts.” The Hague, the Netherlands: The Hague Centre for Strategic Studies, September 2, 2014. https://hcss.nl/report/designing-future-stabilization-efforts.

DeBruyne, Nese F. “American War and Military Operations Casualties: Lists and Statistics.” *Congressional Research Service*, no. RL32492 (April 26, 2017): 38.

Dijsselbloem, Jeroen. Parliamentary Letter. “Toezegging debat Najaarsnota 2015: Defensie-uitgaven.” Parliamentary Letter, January 14, 2016. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/01/14/kamerbrief-defensie-uitgaven/kamerbrief-defensie-uitgaven.pdf.

Dormehl, Luke. “Meet TIKAD: The Gun-Toting Drone That Can Aim, Fire, and Compensate for Recoil.” Digital Trends, August 9, 2017. https://www.digitaltrends.com/cool-tech/duke-gun-robot-tikad/.

Eshel, Tamir. “Soldier Borne Sensors.” *Defense Update* (blog), October 27, 2017. https://defense-update.com/20171027_soldier_borne_sensors.html.

Freedberg Jr., Sydney J. “Miserable, Disobedient & Victorious: Gen. Milley’s Future US Soldier.” *Breaking Defense* (blog), October 5, 2016. https://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/.

Gady, Franz-Stefan. “Meet Russia’s New Killer Robot.” *The Diplomat*, July 21, 2017. https://thediplomat.com/2015/07/meet-russias-new-killer-robot/.

“Global Surveillance Disclosures (2013–present).” *Wikipedia*, July 3, 2018. https://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosures_(2013%E2%80%93present)&oldid=848626139.

Gregg, Heather S. “The Human Domain and Influence Operations in the 21st Century.” *Special Operations Journal* 2, no. 2 (July 2, 2016): 92–105. https://doi.org/10/gdm249.

Hansen, Flemming Splidsboel. “The Weaponization of Information.” DIIS, December 14, 2017. https://www.diis.dk/en/research/the-weaponization-of-information.

Hoffman, F G. “Will War’s Nature Change in the Seventh Military Revolution?,” Winter -2018 2017, 14.

Horowitz, Michael C. “Artificial Intelligence, International Competition, and the Balance of Power.” *Texas National Security Review* (blog), May 15, 2018. https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/.

Jans, Karlijn, and Tim Sweijs. “Monthly Alert: Vital European and Dutch Security Interests | HCSS.” The Hague Centre for Strategic Studies, June 9, 2017. https://hcss.nl/report/monthly-alert-vital-european-and-dutch-security-interests.

Jensen, Benjamin, and Ryan Kendall. “Waze for War: How the Army Can Integrate Artificial Intelligence.” *War on the Rocks* (blog), September 2, 2016. https://warontherocks.com/2016/09/waze-for-war-how-the-army-can-integrate-artificial-intelligence/.

Johansen, Bob. *Get There Early: Sensing the Future to Compete in the Present*. First Edition edition. San Francisco, Calif: Berrett-Koehler Publishers, 2007.

Kahneman, Daniel, and Amos Tversky, eds. *Choices, Values, and Frames*. 1 edition. New York : Cambridge, UK: Cambridge University Press, 2000.

Kania, Elsa. “Battlefield Singularity.” Washington, D.C.: Center for a New American Security, November 2017. https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power.

———. “Swarms at War: Chinese Advances in Swarm Intelligence.” Jamestown, July 6, 2017. https://jamestown.org/program/swarms-war-chinese-advances-swarm-intelligence/.

Lt Gen Deptula, David A. “The St. Andrews Proclamation: A Pragmatic Assessment of 21st Century Airpower,” Mitchell Institute Policy Papers, 12 (June 2018): 16.

Ministerie van Buitenlandse Zaken. “Integrated International Security Strategy 2018-2022.” Rapport, May 14, 2018. https://www.government.nl/documents/reports/2018/05/14/integrated-international-security-strategy-2018-2022.

Ministerie van Defensie. “Defensienota 2018: Investeren in onze mensen, slagkracht en zichtbaarheid.” Beleidsnota. Ministerie van Defensie, March 26, 2018. https://www.defensie.nl/downloads/beleidsnota-s/2018/03/26/defensienota-2018.

———. “Eindrapport Verkenningen 2010 Houvast voor de krijgsmacht van de toekomst.” Report. The Hague, the Netherlands, March 29, 2010. https://www.defensie.nl/downloads/rapporten/2010/03/29/eindrapport-verkenningen-2010.

———. “Strategische Kennis- en Innovatieagenda 2016-2020: Voorblijven in een onveiliger wereld.” Rapport, November 2, 2016. https://www.rijksoverheid.nl/documenten/rapporten/2016/11/02/strategische-kennis-en-innovatieagenda-2016-2020.

National Academies of Sciences, Engineering and Medicine. “Discussion of Selected Topics from the Restricted Report.” In *Counter-Unmanned Aircraft System (CUAS) Capability for Battalion-and-Below Operations: Abbreviated Version of a Restricted Report*, 2018. https://doi.org/10.17226/24747.

NATO. “Framework for Future Alliance Operations.” NATO, 2018. http://www.act.nato.int/images/stories/media/doclibrary/180514_ffao18-txt.pdf.

Nederlandse Grondwet - Artikel 97: Krijgsmacht. Accessed July 2, 2018. https://www.denederlandsegrondwet.nl/id/vkjaj9cxqpwx/artikel_97_krijgsmacht.

Nhan, Johnny, Laura Huey, and Ryan Broll. “Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings.” *The British Journal of Criminology* 57, no. 2 (March 1, 2017): 341–61. https://doi.org/10/gdz3xj.

“RoboValley.” RoboValley. Accessed July 2, 2018. http://www.robovalley.com.

Scharre, Paul. “Robotics on the Battlefield. Part I: Range, Persistence and Daring.” 20YY. Center for a New American Security, May 2014.

———. “Robotics on the Battlefield Part II.” Washington, D.C.: Center for a New American Security, October 2014.

“Service Academies Swarm Challenge Pushes the Boundaries of Autonomous Swarm Capabilities.” DARPA, May 11, 2017. https://www.darpa.mil/news-events/2017-05-11.

Smallwood, David O. “Augustine’s Law Revisited,” March 2012, 2.

Smith, Rupert. *The Utility of Force: The Art of War in the Modern World*. New York: Alfred A. Knopf, 2007.

Søby Kristensen, Kristian. “Military Technology and Small State Strategies.” presented at the Navigating new military technologies: small state strategies for maintaining relevant and effective military forces, Defence Command Denmark Slagelse, May 22, 2018.

“Special Issue ‘Sensors and Sensing in Indoor Localization, Tracking, Navigation and Activity Monitoring.’” *Sensors*, n.d. http://www.mdpi.com/journal/sensors/special_issues/activity_monitoring.

“StatLine.” CBS. Accessed July 3, 2018. https://opendata.cbs.nl/statline#/CBS/nl/.

Sweijs, Tim. “Thinking About the Future of Armed Conflict.” presented at the Presentation Senior Military Leadership Course, The Hague, the Netherlands, March 22, 2018.

Sweijs, Tim, Stephan De Spiegeleire, Karlijn Jans, and Erik Frinking. “Dutch Foreign Relations Index.” The Hague Centre for Strategic Studies, October 19, 2017. https://hcss.nl/report/monthly-alert-dutch-foreign-relations-index.

Telley, Chris, and Samuel Membrere. “Training ‘No Huddle’ Joint Offense.” War on the Rocks, January 31, 2017. https://warontherocks.com/2017/01/training-no-huddle-joint-offense/.

The Economist. “Special Report: Financial Inclusion Is Making Great Strides.” *The Economist*, May 3, 2018. https://www.economist.com/special-report/2018/05/03/financial-inclusion-is-making-great-strides.

The National Network of Safety and Security Analysts. "National Risk Profile 2016: An All Hazard Overview of Potential Disasters and Threats in the Netherlands," 2016.

"The World Factbook — Central Intelligence Agency," 2017. https://www.cia.gov/library/publications/the-world-factbook/.

Toumaj, Amir. "Soleimani's Presence in Aleppo Underscores Strategy of Crushing Rebels | FDD's Long War Journal," September 7, 2016. //www.longwarjournal.org/archives/2016/09/soleimanis-presence-in-aleppo-underscores-strategy-of-crushing-rebels.php.

Tucker, Patrick. "This Tiny Drone Could Transform Urban Warfare." The Fiscal Times, September 12, 2016. http://www.thefiscaltimes.com/2016/09/12/Insect-Sized-Drone-Could-Transform-Urban-Warfare.

———. "US Army Seeks Internet-of-Battlefield-Things, Distributed Bot Swarms." Defense One, July 18, 2017. https://www.defenseone.com/technology/2017/07/us-army-seeks-internet-battlefield-things-distributed-bot-swarms/139533/.

UK Ministry of Defence. "Human-Machine Teaming (JCN 1/18)." Joint Concept Note, May 2018. https://www.gov.uk/government/publications/human-machine-teaming-jcn-118.

———. "Joint Doctrine Publication 04: Understanding and Decision-Making." UK Ministry of Defence, December 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/584177/doctrine_uk_understanding_jdp_04.pdf.

———. "Understanding and Decision Making (JDP 04)." UK Ministry of Defence, December 2010. https://www.gov.uk/government/publications/jdp-04-understanding.

United Kingdom Ministry of Defence. "Deaths in the UK Regular Armed Forces: Annual Summary and Trends over Time 1 January 2008 to 31 December 2017," March 27, 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/694139/20180327_UK_Deaths_National_Statistic_2018_O.pdf.

Ureña, Jesús, Álvaro Hernández Alonso, and Juan Jesús García Domínguez, eds. "Sensors and Sensing in Indoor Localization, Tracking, Navigation and Activity Monitoring." Sensors, no. Special Issue (2018). http://www.mdpi.com/journal/sensors/special_issues/activity_monitoring.

US Army TRADOC. "Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040," December 2017. http://www.tradoc.army.mil/MultiDomainOps/docs/MDB_Evolutionfor21st.pdf.

———. "The U.S. Army Operating Concept 2020-2040," July 2014. https://www.army.mil/e2/c/downloads/367967.pdf.

———. "Threat Tactics Report: Iran." TRADOC, June 2016. https://community.apan.org/cfs-file/__key/docpreview-s/00-00-01-94-15/TTR-Iran-Jun2016.pdf.

US embassy. "US Embassy Cables: Why Holland Is so Important to US." *The Guardian*, December 15, 2010, sec. World news. http://www.theguardian.com/world/us-embassy-cables-documents/38987.

US Joint Chiefs of Staff. "JP 3-05, Special Operations," July 16, 2014, 183.

———. "JP 5-0, Joint Planning," June 16, 2017. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf.

Vincent, James. "Don't Use Huawei Phones, Say Heads of FBI, CIA, and NSA." The Verge, February 14, 2018. https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears.

Waltzman, Rand. "The Weaponization of Information," April 27, 2017. https://www.rand.org/pubs/testimonies/CT473.html.

Weick, K. E. "Management of Organizational Change among Loosely Coupled Elements." In *Change in Organizations*, edited by P. Goodman, 1982.

Wittes, Benjamin, and Gabriella Blum. *The Future of Violence: Robots and Germs, Hackers and Drones—Confronting A New Age of Threat*. New York: Basic Books, 2015.

The Hague Centre for Strategic Studies

info@hcss.nl

hcss.nl

Address:
Lange Voorhout 1
2514EA
The Hague
The Netherlands