2019-12

THE IMPERATIVE SYMBIOTIC RELATIONSHIP BETWEEN SOF AND CYBER: HOW DUTCH SPECIAL OPERATION FORCES CAN SUPPORT CYBER OPERATIONS

van Hooren, Jonas

Monterey, CA; Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

THE IMPERATIVE SYMBIOTIC RELATIONSHIP BETWEEN SOF AND CYBER: HOW DUTCH SPECIAL OPERATION FORCES CAN SUPPORT CYBER OPERATIONS

by

Jonas van Hooren

December 2019

Thesis Advisor:	Ryan Maness
Co-Advisor:	John D. Tullius
Second Reader:	Kalev I. Sepp

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2019	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE
THE IMPERATIVE SYMBIOTIC RELATIONSHIP BETWEEN SOF AND CYBER: HOW DUTCH SPECIAL OPERATION FORCES CAN SUPPORT CYBER OPERATIONS

5. FUNDING NUMBERS

6. AUTHOR(S) Jonas van Hooren

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Dutch SOCOM, Den Haag, Netherlands 2511CR

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release. Distribution is unlimited.

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

As a knowledge-based economy, the Netherlands is vulnerable to digital hybrid threats from state and non-state actors. The Dutch strategic military leadership sees the importance of improving its digital defense, but struggles with the right approach. This research, based on a heuristic method including literature reviews and interviews, provides an answer to the question, "How can Dutch Special Operations Forces (SOF) enhance the national cyber capabilities to counter the hybrid threats that the Netherlands currently faces?" by offering three options: 1) SOF can gain access to hard targets for cyber operations; 2) it can provide the means to get wetware, hardware, and software in or out the operation area; and 3) it can understand, deceive, and influence the cultural environment. Furthermore, the thesis provides the Dutch Ministry of Defense three potential integration options for SOF and cyber capabilities. The ministry can 1) delegate cyber-SOF teams to the operational commands; 2) embed SOF and cyber personnel in each other's organizations; and 3) create a new cyber-enabled special operations unit. With the new Special Operations Command, the Defense Cyber Command, and the Joint SIGINT Cyber Unit, there are opportunities for SOF to support cyber operations and increase the digital security for the Netherlands and its NATO allies.

14. SUBJECT TERMS
composite special operations command, cyber supporting operations, cyber terrorism, defense cyber command, ministry of defense, hackers, hacktivists, hybrid threat, hybrid warfare, offensive cyber operations, information warfare, intelligence, irregular warfare, secret services, special operations command, special operations forces, strategic implications, technology, the Netherlands, unconventional warfare

15. NUMBER OF PAGES
125

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

THE IMPERATIVE SYMBIOTIC RELATIONSHIP BETWEEN SOF AND CYBER: HOW DUTCH SPECIAL OPERATION FORCES CAN SUPPORT CYBER OPERATIONS

Jonas van Hooren
Major, Netherlands Marine Corps
BEc, Nederlands Talen Instituut, 2008

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN DEFENSE ANALYSIS
(IRREGULAR WARFARE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2019**

Approved by: Ryan Maness
Advisor

John D. Tullius
Co-Advisor

Kalev I. Sepp
Second Reader

Kalev I. Sepp
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As a knowledge-based economy, the Netherlands is vulnerable to digital hybrid threats from state and non-state actors. The Dutch strategic military leadership sees the importance of improving its digital defense, but struggles with the right approach. This research, based on a heuristic method including literature reviews and interviews, provides an answer to the question, "How can Dutch Special Operations Forces (SOF) enhance the national cyber capabilities to counter the hybrid threats that the Netherlands currently faces?" by offering three options: 1) SOF can gain access to hard targets for cyber operations; 2) it can provide the means to get wetware, hardware, and software in or out the operation area; and 3) it can understand, deceive, and influence the cultural environment. Furthermore, the thesis provides the Dutch Ministry of Defense three potential integration options for SOF and cyber capabilities. The ministry can 1) delegate cyber-SOF teams to the operational commands; 2) embed SOF and cyber personnel in each other's organizations; and 3) create a new cyber-enabled special operations unit. With the new Special Operations Command, the Defense Cyber Command, and the Joint SIGINT Cyber Unit, there are opportunities for SOF to support cyber operations and increase the digital security for the Netherlands and its NATO allies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

C2	Command and Control
CCDCOE	Cooperative Cyber Defense Centre of Excellence
CCIR	Commander Critical Information Requirement
CHOD	Chief Of Defense (The Netherlands)
COM	Commander
COTS	Commercial Off The Shelf
CIA	Central Intelligence Agency (the United States)
CSOC	Cyber Special Operation Command (United States)
C-SOCC	Composite Special Operations Component Command (NATO)
CT	Counter Terrorism
DA	Direct Action
DCC	Defensive Cyber Command (the Netherlands)
DIME	Diplomatic, Information, Military, and Economic
DPD	Diver Propulsion Device
DoD	Department of Defense (the United States)
EU	European Union
FBI	Federal Bureau of Investigations (the United States)
FOB	Forward Operating Base
FP	Force Protection
FRINGE	Photo, Robo, Info, Nano, Geno, and Electro
GISS	General Intelligence and Security Service (the Netherlands)
GRU	*Glavnoje Razvedyvatel' noje Upravlenije* (military intelligence directorate Russia)
HAHO	High-Altitude High-Opening
HALO	High-Altitude Low-Opening
HUMINT	Human Intelligence
ICT	Information and Communications Technology
IPE	Intelligence Preparation of the Environment
IoT	Internet of Things
IRB	Institutional Review Board
ISR	Intelligence, Surveillance, and Reconnaissance
ISIS	Islamic States of Iraq and the Levant

JIVC	Joint Information Provision Commando
JSCU	Joint SIGINT Cyber Unit (the Netherlands)
KCT	*Korps Commando Troepen* (Army SOF the Netherlands)
MA	Military Assistance
MARSOF	Maritime Special Operation Forces (Maritime SOF the Netherlands)
MISS	Military Intelligence and Security Service (the Netherlands)
MKSO	*Ministeriële Kerngoep Speciale Operaties* (Ministrial Core Group Special Operations)
MoD	Ministry of Defense (the Netherlands)
NATO	North Atlantic Treaty Organization
NCTV	National Coordinator for Security and Counterterrorism (The Netherlands)
NGO	Non-Governmental Organization
NLMARSOF	Netherlands Maritime Special Operations Forces
NRF	NATO Response Force
NSA	National Security Agency (the United States
NSHQ	NATO SOF Headquarter
OCO	Offensive Cyber Operations
OPCO	Operational Command
OPCW	Organization for the Prohibition of Chemical Weapons
OSINT	Open Source Intelligence
QRF	Quick Reaction Force
ROE	Rules Of Engagement
SDMP	Special Decision Making Process
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	Signal Intelligence
SOCOM	Special Operations Command
SOF	Special Operations Forces
SOMTG	Special Operations Maritime Task Group
SR	Special Reconnaissance
TACOM	Tactical Command
TACON	Tactical Control

TSE	Tactical Sight Exploitation
TTP	Tactics, Techniques, and Procedures
UN	United Nations
WIV	*Wet Inlichtingen & Veiligheid* (Law on Intelligence & Security)

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

As a small European state, the Netherlands is in many ways a very safe country, but the world's security situation is changing rapidly. The increasing hybrid threats, including cyber-attacks, combined with the new Dutch Special Operation Command and Defense Cyber Command planted the seed for this thesis. After various fruitful discussions with Professor John Arquilla, the seed germinated. The Naval Postgraduate School (NPS), with the Defense Analysis Department, in particular, provided me the opportunity to grow that germ seed into a master's thesis.

Therefore, I would like to express my sincere gratitude to my advisors, Ryan Maness, John Tullius, and Kalev I. Sepp, for their useful and extensive remarks, engagement, comments, and discussions throughout this process. But also, I would like to acknowledge the other NPS professors with whom I consulted frequently during the thesis process, such as, Camber Warren, Dorothy Denning, Douglas Borer, Eric Jansen, Gordon McCormick, Ian Rice, and my favorite writing coach, Colette O'Connor.

I also want to thank individuals outside of NPS. I am grateful to those who allowed me to pitch ideas for my thesis, such as Harvard professor Max Smeets, internet entrepreneurs (and neighbors) Mike Eynon and his wife, Laura, researcher Sergei Boeke, Fox-IT research director Paul Muis, the Knowledge & Innovation Centre Dutch SOCOM with Lieutenant-Colonel George Dimitriu and scientific officer Funs Titulaer, NSHQ professor Doug Overdeer, and the various SOF and cyber colleagues from U.S. and Dutch military organizations.

Additionally, I wish to thank the interviewees I spoke with in the Netherlands or via Skype: Commander Dutch SOCOM Major-General ten Haaf, Commander Dutch Defense Cyber Command Commodore Boekholt O'Sullivan, Commander Joint SIGINT Cyber Unit Marc Brinkman, Defense cyber expert Jelle Haaster, operational manager crypto Fox-IT Daniël Datau, director crypto Fox-IT Jurgen Delfos, Commander NLMARSOF Lieutenant-Colonel Jan-Willem van Dijk, and Commander KCT Colonel Rene van den Berg.

Last but certainly not least, I wish to thank my beautiful wife, Sara, who agreed to join me in this California adventure, who endured my academic endeavors the last 18 months, and more importantly, is the love of my life and an excellent mother of our three lovely children.

I. INTRODUCTION

> Where a small country can stand out: Innovation as the engine of the Dutch knowledge economy with a testing ground for mobility, IT, wind energy, and climate adaptation.
>
> —Global Innovation Index 2018[1,2]

A. PROLOGUE

On the sunny morning of April 11, 2018, Russian cyber operator Aleksej Sergejvitsj Morenets left the military main intelligence directorate GRU (Glavnoje Razvedyvatel' noje Upravlenije) headquarters in Moscow to take a taxi to the airport. In the airport, he joined his cyber colleague Yevgeni Michajlovitsj Serebrakov and two support agents—Oleg Miajlovitsj Sotnikov and Alexej Valerjevitsj Minin—from the GRU intelligence cyber warfare team, also known as ATP 28 or Unit 26165. Together they traveled on diplomatic passports on a direct flight from Moscow to Amsterdam with one mission: hack the world's top chemical weapons watchdog in The Hague, the Organization for the Prohibition of Chemical Weapons (OPCW).[3]

After the recent nerve gas poisoning of Russian ex-spy Sergei Skripal and his daughter in the British city of Salisbury, and the chemical attack by Syria's Russian-backed military in Douma, the OPCW launched extensive investigations. The OPCW blamed Russia, with evidence leading to the Russian GRU being the culprit. Russia protested that the OPCW was going far beyond its mandate, and did not wait for the OPCW results, but sent their GRU hackers to the Netherlands.

---

[1] Soumitra Dutta, Bruno Lanvin, and Sacha Wunsch-Vincent, *Global Innovation Index 2018: Energizing the World with Innovation*, 11th ed., Cornell University, INSEAD, and the World Intellectual Property Organization (Geneva, Switzerland: World Intellectual Property Organization, 2018), https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018.pdf.

[2] The Netherlands became number two (after Switzerland) in the Global Innovation Index 2018.

[3] "How the Dutch Foiled Russian 'Cyber-Attack' on OPCW," BBC News, October 4, 2018, https://www.bbc.com/news/world-europe-45747472.

After arriving in the Netherlands, the GRU cyber warfare team hired a car and scouted the OPCW building and the surroundings to prepare for a closed access hack on the OPCW's Wi-Fi network. On April 14, during the attempt, the rental car fully packed with state-of-the-art hacking equipment was in the parking lot of the Marriott hotel, as close as possible to the neighboring OPCW building. From the moment the GRU team set foot on Dutch ground, however, they were closely monitored by the Dutch military intelligence and security services (MISS). Before the actual hack, whose purpose was to compromise and disrupt OPCW computers, the GRU team was intercepted and detained by Dutch authorities, who were prepared to prevent a cyber-attack against the OPCW. The GRU team tried to destroy one of their Russian cellphones, which showed their heightened awareness of security. After having all of their technical hacking equipment, laptops, antennas, cameras, and mobile telephones confiscated, they were escorted to Schiphol Airport and deported to Moscow, without any of their hacking tools.[4] [5]

This discovery of the failed Russian hacking operation in The Hague shows that the Netherland's knowledge, innovation, network, and technology services arouse interest and are possibly vulnerable to virtual and physical (hybrid) threats instigated by foreign organizations and institutions.

B. BACKGROUND TO THE PROBLEM

The Netherlands is in many ways a very safe country, but the world's security situation is changing rapidly. The general feeling about the safety in and around the Netherlands has deteriorated, and the associated risks have increased and affected the national security situation. Geopolitical and economic power shifts, instability and insecurity around Europe and the Caribbean part of the Kingdom of the Netherlands—with Venezuela as a close regional neighbor—have accelerated technological development and increased both hybrid conflict and tensions within the Netherlands and Europe. All of these

---

[4] "NRC: Russische ambassade is spionagecentrum, was betrokken bij poging OPCW binnen te dringen," [Russian embassy is espionage center, and was involved in intended penetration OPCW], *de Volkskrant*, December 1, 2018, https://www.volkskrant.nl/nieuws-achtergrond/nrc-russische-ambassade-is-spionagecentrum-was-betrokken-bij-poging-opcw-binnen-te-dringen~bb9402dc/.

[5] All translations from Dutch to English are, unless otherwise noted, the author's own translations.

developments have increasingly affected Dutch security.[6] Multiple cyber-incidents, plus the shooting down of flight MH17 above Ukrainian territory in July 2014 (which resulted in the deaths of 196 Dutch citizens), made it clear that many disruptions in the world have a direct or indirect impact on the Netherlands. Moreover, the arrival of refugees in the Netherlands, as a result of civil wars in the Middle East and Africa, the struggle with the Islamic States of Iraq and the Levant (ISIS) in Syria and Iraq, as well as the ISIS-linked examples of unwanted foreign interference and terrorist threats, like the recent tram terror attack in Utrecht,[7] dramatically illustrate this impact. The current Dutch threat level is "substantial"—that is, level 4 on a scale of 1 to 5.[8] The threats posed by terrorist attacks, cyber-attacks, unwanted foreign interference and undermined elections, military pressure, and attacks on critical economic processes are urgent and require an effective holistic security policy.

While tangible threats, like terrorist acts, take place in the physical domain, other threats happen in the virtual domain, such as cyber threats via hacking and misinformation, which are less predictable and understandable. Recently, the Russian GRU's attempted hacking of the OPCW in The Hague has clearly shown that the Netherlands as an information, innovation, and technology state hosting various international organizations[9]—including not only the OPCW, but the International Criminal Court, Interpol, EU, the North Atlantic Treaty Organization (NATO), and United Nations (UN)

---

[6] Ministerie van Buitenlandse Zaken, *Wereldwijd voor een Veilig Nederland: Geïntegreerde Buitenland- en Veiligheidsstrategie 2018–2022* [Worldwide a Secure Netherlands: Integrated Foreign and Security Strategy 2018–2022] (The Hague: Ministerie van Buitenlandse Zaken, 2018), https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs.

[7] Robin Simcox, "The Netherlands' Luck Is Running Out," *Foreign Policy*, March 25, 2019, https://foreignpolicy.com/2019/03/25/the-netherlands-luck-is-running-out/.

[8] "Attack in Utrecht and Arrests Confirm Threat," National Coordinator for Security and Counterterrorism, July 4, 2019, https://english.nctv.nl/latest/news/2019/07/04/attack-in-utrecht-and-arrests-confirm-threat.

[9] The Netherlands hosts more than 40 various international organizations, mostly located in and around The Hague. *See* https://www.rijksoverheid.nl/onderwerpen/internationale-organisaties-in-nederland/lijst-van-internationale-organisaties-in-nederland.

institutions—and thus, is vulnerable to cyber-threats.[10] Conflicts elsewhere in the physical and virtual environment have an impact in the Netherlands. The *Dutch Cyber-security Picture 2018* describes espionage, sabotage, and disruption by states as the most significant threats for the country's national security.[11] The same high-speed networks used by the Dutch population to share information, work, text, and shop, are also used by others to spy and attack.[12]

The Dutch Scientific Council for Government Policy argues that security can no longer be found in a physical bulwark against aggression from outside, but requires policy based on insights into the many connections between "inside" and "outside" the Netherlands.[13] Therefore, the Netherlands might develop a more integrated inter-department approach in its security strategy, so that the ends, ways, means, and risks are balanced in today's world of connectedness.[14] Essentially, this security strategy would be comprehensive and provide direction to the Dutch Ministry of Defense (MoD). Its purpose would be to mitigate the risks and control the ways and means to achieve these ends. To accomplish this goal, a safe and secure cyber strategy is required, including sufficient power to govern. This power would be divided into political, diplomatic, economic, military, and informational

---

[10] Wendelmoet Boersema, "Wat we Weten over de Russische Hackaanval tegen de OPCW" [What We Know about the Russian Hack against the OPCW]," *Trouw*, October 4, 2018, https://www.trouw.nl/home/wat-we-weten-over-de-russische-hackaanval-tegen-de-opcw~ad2eb078/.

[11] "Cyber Security Assessment Netherlands CSAN 2018," National Coordinator for Security and Counterterrorism. Ministry of Justice and Security, 2019, https://english.nctv.nl/documents/publications/2018/08/07/cyber-security-assessment-netherlands-2018

[12] Huib Modderkolk, *Het is Oorlog maar Niemand die het Ziet*, [It is War but Nobody Sees it], 3rd ed (Publisher Podium, Amsterdam, 2019), 22, http://www.letterenfonds.nl/nl/boek/1273/het-is-oorlog-maar-niemand-die-het-ziet.

[13] Department for Public Law, Jurisprudence and Legal History, *Veiligheid in een Wereld van Verbindingen: Een Strategische Visie op het Defensiebeleid* [Security in a World of Connections: A Strategic Vision of Defense Policy], WRR-Rapport nr. 98 (The Hague: WRR, 2017), https://research.tilburguniversity.edu/en/publications/82b3474a-edac-4a9e-97d6-af3a0807e17d.

[14] David Kilcullen, *Out of the Mountains: The Coming Age of the Urban Guerrilla* (Oxford; New York: Oxford University Press, 2013).

environments.[15] Domestic and foreign (security) politics must cooperate, balance, and reinforce each other in technologies, doctrines, and information to make a combined fist against hybrid threats.

The Dutch government needs to coordinate its international relations, which requires strategic analysis of the current security situation. This should combine the internal and external security policy, defense policy, and, in particular, the role of the armed forces in the Dutch MoD. Based on these intertwined relationships, all of which affect the internal and external security of the Netherlands, Dutch politicians acknowledge that an active foreign policy in support of national interest is vital.[16]

The weakening of the international security situation, combined with the intensifying geopolitical conflicts of interest, makes the Dutch Defense's involvement in cyber security critical. The cyber-domain has made it possible for malicious actors to steal Dutch intellectual property without the perpetrators being physically in the Netherlands. The MoD aims to counter these threats. Moreover, the increasingly digitized country must prepare for "advanced digital threats in the event of an unforeseen (military) conflict." [17] The Defense organization has a responsibility to assume that this could happen (or has already happened), both at the national level with its intertwined relationship with other departments or national instruments of power, and on the international level through membership in NATO and other international organizations.[18]

The OPCW hacking example, in April 2018, provides food for thought and possible opportunities for actual improvements to be made by the Dutch authorities and the MoD,

---

[15] Harry R. Yarger, "Towards a Theory of Strategy: Art Lykke and the Army War College Strategy Model," in *Guide to National Security Policy and Strategy*, vol. 2 (Carlisle, PA: U.S. Army War College, 2006), 107–13, https://catalyst.library.jhu.edu/catalog/bib_2801120.

[16] Jacques J. A. Thomassen, Kees Aarts, and Hendrik van der Kolk, eds., *Politieke Veranderingen in Nederland 1971–1998: Kiezers en de Smalle Marges van de Politiek* [Political Changes in the Netherlands 1971–1998: Voters and the Narrow Margins of Politics] (The Hague: SDU Uitgevers, 2000), https://research.utwente.nl/experts/en/publications/13ce06d6-a53e-435e-9a06-4b94942bff82.

[17] Dutch Ministry of Defense, "The Netherlands Armed Forces Doctrine for Military Cyberspace Operations" (The Hague: Dutch Defense Cyber Command, February 2019).

[18] Dutch Ministry of Defense.

in particular. Physical actions by the GRU in the Netherlands in combination with virtual activities online demand a similar approach: combine capabilities and efforts in the virtual world with the physical world and vice versa. Various MoD specialists from intelligence, cyber, and Special Operation Forces (SOF), often working in a stovepipe manner, should focus on their branch as well as collaborate against hybrid threats. With the recent establishment of the Netherlands Special Operations Command (NLD SOCOM), the MoD has increased the planning capacity of special operations in the growing hybrid conflicts.[19] In combination with the possible strategic utility of SOF as information collectors to support national decision-making[20] and the uprising of the Defense Cyber Command (DCC) in close cooperation with the more mature and experienced Joint SIGINT Cyber Unit (JSCU), there are opportunities to make that joined inter-agency fist against the current hybrid threats.

C. PURPOSE AND SCOPE

This thesis aims to investigate the potentially crucial symbiotic relationship between SOF and cyber capabilities within the military national instrument of power at the strategic level and its impact on the operational and tactical levels of hybrid conflict. Specifically, it aims to investigate the relation and coordination between the physical environment, where SOF operates, and the more abstract virtual environment, the cyber domain. If these two environments are effectively connected, this combination could lead to synergy and provide the MoD with better insights into more efficient and effective capabilities to prepare against both national and international hybrid threats the Netherlands may have to deal with.

Cyber-space is a boundless domain, and it grows in complexity and capacity every day. To define the scope of this thesis, the research focuses on the military offensive,

---

19 *Special Operations Forces: Schaduwkrijgers in Het Licht van de Toekomst* [Special Operations Forces: Shadow Warriors in The Light of the Future] (The Hague: The Hague Centre for Strategic Studies, 2015), https://hcss.nl/report/special-operations-forces-schaduwkrijgers-het-licht-van-de-toekomst.

20 B. Haspels and F. Elkjaer Haar, "The Strategic Utility of Small-States Special Operations Forces (SOF) as Information Collectors to Support National Decision-making," (master's thesis, Naval Postgraduate School, 2019).

defensive, and intelligence exploitation components in the cyber realm, and how these components can be exploited during physical SOF operations. Moreover, the study explores the possible roles SOF can play to support the various cyber operations. The goal would be that both SOF and cyber can innovate, reinforce, and learn together to be more effective. Although the primary focus centers on the SOF and cyber capabilities from the Netherlands' perspective, there is the wider goal: this thesis will also be useful to a broader audience. Due to the newly formed Dutch SOCOM and its intent to form a Composite Special Operations Component Command (C-SOCC) with Belgium and Denmark, this thesis could be used for NATO SOF and their cyber capabilities as well. In 2021, the C-SOCC will be fully operational and will participate in the NATO Response Force (NRF) to support alliances and other operations. Therefore, the outcomes and recommendations for the Netherlands could also be useful for NATO SOF represented by the NATO SOF Headquarters (NSHQ) at Supreme Headquarters Allied Powers Europe (SHAPE), in Belgium, and for the multinational and interdisciplinary NATO Cooperative Cyber Defense Centre of Excellence (CCDCE) in Tallinn, Estonia.

D. RESEARCH QUESTIONS

In the Netherlands, senior-level military and civil officials are searching for the best ways to integrate SOF and cyber-means to be more effective against adverse hybrid threats (ends). With the recent establishment of NLD SOCOM (December 2018) and the expansion of military cyber capabilities inside the DCC and JSCU, the research question is:

- How can Dutch Special Operations Forces enhance the national cyber capabilities to counter the hybrid threats the Netherlands currently faces?

This principal research question is supported by other questions, which are placed in a logic trail. In short, every answered question will lead to a new follow-up question to clarify the research question of this thesis. Before talking about Dutch SOF or cyber operations, first the national and international hybrid threats the Netherlands currently faces must be explained. Next, it is important to determine whether the Netherlands has sufficient means, such as cyber capabilities, to counter these hybrid threats. If the answer

to this question is negative, then the principal research question can be further explored: Should Dutch SOF have a role to play filling these cyber gaps? If the answer is positive, the following logical question is what are the potential roles and capabilities of Dutch SOF in the cyber domain? If Dutch SOF have a role to play in the cyber realm, it is important to investigate how SOF and cyber operations could be integrated into the Dutch national security strategy. This is followed by the question, what would be the tactical and operational effects for this integration? Finally, this thesis provides some conclusions and recommendations for SOF's role in the cyber domain and focuses on the NATO level to answer the question as to how NATO SOF and cyber operations can be integrated into the first C-SOCC with Belgium, Denmark, and the Netherlands.

E. CHAPTER OUTLINE

After the description of the thesis topic its scope, and purpose, as well as the introduction of the research question and to the problem itself for the Netherlands, presented in this first chapter, the remainder of this thesis is organized as follows: Chapter II focuses on the literature review and the methodology used in this study. This chapter also reviews literature related to both SOF and cyber operations, and explains how the heuristic methodology is used in this thesis. Chapter III offers an in-depth examination of the hybrid threat for the Netherlands and the challenges for Dutch cyber organizations, along with their capabilities to address these challenges. Next, Chapter III examines the Dutch SOF's options that can support cyber operations to tackle these hybrid threats. Chapter IV analyzes the integration possibilities of the Dutch SOF and cyber capabilities, while it also addresses the challenges of this integration. Finally, Chapter V provides the author's conclusions, recommendations, and suggestions for future C-SOCC and NATO cyber SOF integration. The final chapter also recommends areas for further inquiry and research.

II. LITERATURE REVIEW AND METHODOLOGY

> As tomorrow's character of conflicts continues to rapidly digitize, the space between the virtual world and physical world will shrink.
>
> —Colonel Patrick Michael Duggan[21]

A. LITERATURE REVIEW

Computers are everywhere and we rely on them every day. We are surrounded by machines, even if we do not recognize them immediately as machines. From the moment we wake up until the moment we go to bed, we use computers to help, understand, communicate, measure, calculate, interpret, and evaluate our daily lives as we sleep, eat, exercise, commute, work, and relax—all in an effort to be productive, active, healthy, and efficient. Socially, we are devoted to this digital infrastructure. All these infrastructures are connected via the Internet of Things (IoT) and communicate in the cyber domain. At the same time, this cyber domain creates opportunities as well as vulnerabilities related to safety and security in the Information Age.[22]

These opportunities and vulnerabilities in the network of computers were already forecast by cyber-security researchers John Arquilla and David Ronfeldt in 1993.[23] Their term "cyberwar" was born and used as an operational concept to control and translate information dominance into battlespace dominance. Senior political cyber-analyst Martin Libicki builds on this term and describes cyberwar as when "a state believes it could gain

---

[21] Unconventional Cyber, COL Pat Duggan, "The Unconventional Use of Cyber between War and Peace," produced by Georgetown University, video, 0:06, accessed May 24, 2019, https://www.youtube.com/watch?v=IFEE_nr8kYM.

[22] P. W. Singer, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford; New York: Oxford University Press, 2014).

[23] John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (April 1, 1993): 141.

advantages over another state by stealing, disrupting or manipulating the information systems through deliberate provocation or through escalation."[24]

Cyberwar, or the less inflammatory terms cyber conflict or cyber competition, could trigger a reaction in the physical domain. Virtual deterrence or a cyberwar act could have physical consequences; a correlation thus exists between actions in the virtual domain and reactions in the physical domain and vice versa. Examples of this correlation are the Siberian gas pipeline explosion in 2004, the Stuxnet attack developed in 2005 targeting the centrifuges of the Iranian nuclear plant but unnoticed until 2010, the paralysis of the financial system in Estonia in 2007, the first real use of cyber capabilities by Russia in the war in Georgia in 2008, the Russian annexation of Crimea with a combination of cyber and physical military means in 2014, and more recently, the interference in the U.S. elections in 2016.[25] All these incidents were triggered online by cyber experts and illustrate how objects and events were consequently influenced, manipulated, disrupted, damaged, or even broken in the physical world. The Siberian gas pipeline infrastructure was virtually manipulated, which resulted in a physical sabotage: an over-pressed gas pipeline explosion. The U.S.-Israeli digital worm Stuxnet attacked the Iranian nuclear enrichment facilities by manipulating its control program to sabotage the spinning frequency of the nuclear enrichment centrifuges.[26] The Stuxnet attack was probably the first used offensive cyber weapon,[27] and delayed Iranian nuclear development for years. Estonia's heavy reliance on digital infrastructure, which was hacked by Russia, resulted in closed banks, closed

---

[24] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), https://www.rand.org/pubs/monographs/MG877.html.

[25] Brandon Valeriano and Ryan Maness, "The Fog of Cyberwar: Why the Threat Doesn't Live Up to the Hype," *Foreign Affairs*, November 21, 2012, https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar.

[26] Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations* (Oxford; New York: Oxford University Press, 2017), 31–33, https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012.

[27] Lorenzo Franceschi-Bicchierai, "The History of Stuxnet: The World's First True Cyberweapon - VICE," Vice News, August 9, 2016, https://www.vice.com/en_us/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee.

ministries, closed news organizations, and even a closed parliament.[28] The Georgian battlefield was well prepared by Russian online influence operations, which paved the way for the physical military troops to enter.[29] Russia did the same during the annexation of Crimea.[30] Despite there being no military battle in the United States, more and more facts from the ongoing investigation show that the 2016 presidential election was at least influenced by online Russian trolls sending misinformation through fake social media accounts.[31]

Due to various societal and technological changes concomitant with the Information Age, such as the dominance of the Internet of Things, the more interconnected world, and faster and better networks, the traditional operational environments (land, maritime, air, and space domain) have been enriched and, at the same time, imperiled by a new environment: the information environment. Cyberspace is a part of that information environment. Hence, the current environments in which armed forces deploy their assets can be divided into five domains: sea, land, air, space, and cyber.[32] The cyber, or "fifth," domain encompasses all forms of "digital warfare."[33] Like the other four domains, cyber has specific characteristics that help to determine how a means of power could be used.

Yet, the cyber domain differs from the other domains in that it is a human-made, partly non-physical domain. Cyberspace virtually crosses the other domains' physically delineated boundaries. Cyberspace consists of physical components such as computers, servers, routers, satellites, and cables on the land, sea, in the air, and space. In turn, these

---

[28] Tim Maurer, *Cyber Mercenaries: The State, Hackers, and Power* (Cambridge, UK: Cambridge University Press, 2018), 97–98, https://carnegieendowment.org/2018/01/18/cyber-mercenaries-state-hackers-and-power-pub-75280.

[29] Maurer, 101–2.

[30] Maurer, 98–100.

[31] "2016 Presidential Campaign Hacking Fast Facts," CNN, October 18, 2019, https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

[32] The current Netherlands Defence Doctrine still mentions 'Information Domain (incl. Cyber)' as a fifth domain.

[33] Digital warfare is defined as any activity involving the use of computer code / data stream to achieve military objectives, according to the Dutch Defence Cyber Strategy 2019.

traditional fields can function effectively through cyberspace. Consequently, the five domains are dynamically interlinked; a change in one area usually has implications for the situation impacting the others.[34] U.S. Air Force Major General Sam Barret characterizes cyberspace as a global common,[35] like the world's seas and waterways. Just like space, air and oceans, cyberspace does not have boundaries and exists outside sovereign jurisdictions. Hence, online and physical security start slowly to converge.

The lack of boundaries and sovereign jurisdictions can make the cyber domain an environment of lawlessness and could facilitate criminality and terrorism. Therefore, it is important to make rules and regulations about responsible behavior in global, shared cyberspace. According to the 2017 U.S. National Security Strategy, "Access to these shared spaces is at risk due to increased competition and provocative behaviors."[36] No individual country has absolute sovereignty, but all countries agree on best behaviors to protect these areas, just as they do for the Arctic and Antarctic.

Cyberspace can be considered to be interconnected and "autonomous physical or virtual networks, software-controlled systems or devices, software, and data."[37] Therefore, cyberspace goes beyond the Internet and everything that is connected to it, and thus includes digital hardware or systems that are not connected. Based on the U.S. military dictionary, professor Scott Jasper defines cyberspace as "a global domain within the

---

[34] Ministry of Defense, *Defensie Cyber Strategie 2018: Inversteren in Digitale Slagkracht voor Nederland* [Defense Cyber Strategy 2018: Investing in Digital Power for the Netherlands], (The Hague: Ministry of Defense, 2018), https://www.thehaguesecuritydelta.com/media/com_hsd/report/214/document/web-Brochure-Defensie-Cyber-Strategie.pdf."

[35] Bastian Giegerich et al., *Managing Change: NATO's Partnerships and Deterrence in a Globalised World*, ed. Riccardo Alcaro and Sonia Lucarelli (Villa GuastaVillani, Bolonna, Italy: NATO Supreme Allied Command Transformation, 2011), http://www.act.nato.int/images/stories/events/2011/managing_change_hr.pdf.

[36] Department of Homeland Security, *National Security Strategy of the United States of America 2017* (Washington, DC: Department of Homeland Security, 2017), 32, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[37] Gorkem Yigit and Dana Cooperson, *From Autonomous to Adaptive: The Next Evolution in Networking* (Siena: Analysys Mason 2018), https://www.ciena.com/insights/white-papers/From-Autonomous-to-Adaptive-The-Next-Evolution-in-Networking.html.

information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[38] Dutch cyber researcher Jelle Haaster defines cyberspace simply as virtual software plus physical hardware linked by the human user in a networked environment.[39]

Cyberspace influences the future of the military and will especially affect SOF, because both worlds are coming closer together. The difference between soldiers using real guns and hackers pulling the trigger online will get more diffuse.[40] Automated algorithms designed to engage in combat without direct human intervention or oversight, for example, would be a perfect tool for a hacker to turn an armed force against itself. Hacking one enemy to attack another enemy without the instigator even entering the physical war area—all while claiming plausible deniability—is now a potential threat. The physical role SOF plays in hybrid warfare will necessarily evolve when future hybrid warfare will mostly happen online.

B. THE ROLES OF SOF AND CYBER IN EACH OTHER'S DOMAINS

Scholars and strategists, including Eric Trias and Bryan Bell, have identified similarities between special operations and cyber operations. They write: "The inherently clandestine nature of special operations parallels the ease of conducting stealthy cyber operations."[41] Patrick M. Duggan, a retired Special Forces Colonel, proposes that "cyber warfare is, at its core, human-warfare" and "requires SOF's unique human expertise,

---

[38] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (London: Rowman & Littlefield, 2017).

[39] Jelle Haaster, "De Toekomst van de Landmacht met Jelle Haaster" [The Future of the Dutch Army with Jelle Haaster], HCSS Podcast, 0:12, accessed March 3, 2019, https://podcasts.apple.com/us/podcast/hcss-podcast-toekomst-van-landmacht-met-jelle-van-haaster/id1274061866?i=1000427791939.

[40] Hans Bustra, *Security Leaks for Sale*, Zero Days VPRO Tegenlicht (VPRO, 2014), https://www.youtube.com/watch?v=JhkXSg9KQE8.

[41] Eric D. Trias and Bryan M. Bell, "'Cyber This, Cyber That . . . So What?,'" *Air & Space Power Journal* 24, no. 1 (Spring 2010): 95.

unconventional mindsets, and discreet asymmetric options."[42] As more machine learning and deep learning find their way into cyber, Duggan sees "cyber-enabled special warfare as the answer for hybrid threats in an increasingly interconnected global environment in which physical infrastructure is rapidly being assigned."[43] According to the technology editor for *Defense One*, Patrick Tucker, in 2020, over 50 billion machine-to-machine devices will connect to cyberspace by "the embedding of computers, sensors, and Internet capabilities."[44] Currently, 95% of warfighting is traditional warfighting consisting of tanks, planes, and ships, and only 5% is taking place in the cyber-domain; however, the expectations are that within the next ten or 15 years, the ratio will change to 50–50.[45] Cyber-enabled special warfare operators, like the combination of Russian Spetsnaz with cyber experts, who seized Crimea in 2014,[46] "could bridge the gap between the virtual and the physical domains by harnessing modern-day information networks and melding them with old-fashioned, face-to-face SOF partner engagement."[47] As stated by Mike Eynon, co-founder and president of the U.S. cyber-security company Silver Tail Systems, "at the end of the day, in 99% of the hacks I have ever seen in my more than twenty years I have been working in (non-military) cyber security, a human is still the best person to recognize an attack and act in the most appropriate manner."[48]

---

[42] Patrick Michael Duggan, "Strategic Development of Special Warfare in Cyberspace," *Joint Force Quarterly* 4th Quarter, no. 79 (October 2015), https://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyberspace/.

[43] Duggan.

[44] Patrick Tucker, "The CIA Fears the Internet of Things," *Defense One*, accessed February 13, 2019, https://www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/.

[45] Miladinova et al., *Special Operations Forces: Schaduwkrijgers in Het Licht van de Toekomst*.

[46] "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks" The Henry M. Jackson School of International Studies, accessed July 22, 2019, https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

[47] Patrick Michael Duggan, "'Why Special Operations Forces in U.S. Cyber-Warfare?'" *Cyber Defense Review*, January 8, 2016, https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136057/why-special-operations-forces-in-us-cyber-warfare/.

[48] President of Silver Tail Systems Mike Eynon, email message to author, June 2, 2019.

Former U.S. Special Operations Command (USSOCCOM) Commander General Joseph L. Votel stated to the U.S. Congress, "Cyber threats are an increasingly common component of unconventional strategies for which we must develop a more comprehensive approach ... it is time to for us to have an in-depth discussion on how we can best support our national interests in these situations."[49] Special Operations Forces are specially selected, trained, and equipped for ambiguous conflicts everywhere in the world.[50] In accordance with the NATO doctrine *Allied Joint Publication 3.5*, SOF is able to conduct Special Reconnaissance (SR), Military Assistance (MA), and Direct Action (DA) missions.[51] These three main tasks, or derivatives of these, are originally executed in the physical landscape. On the other hand, the cyber domain gives SOF opportunities to counter hybrid threats and validate the proposed data and actions in the physical areas that are communicated through cyber. The cyber domain gives nation-states the opportunity to counter under the radar, and SOF could be a proficient capability to support these cyber acts against national threats. Duggan goes a step further: "SOF could be the perfect tool against hybrid threats inside the physical domain.… SOF could be the discreet human connector from the Defense cyber desk-officer back in the home country to the adversaries in the cyber gray zone."[52] SOF could be the global human link between the physical environment and the virtual online cyber-domain. Being physically on the ground gives SOF opportunities to establish relations and connections with local stakeholders, which cyber operations could benefit from. Duggan put it in another way:

> SOF are the key to humans in cyberwarfare and deception, and manipulation. SOF can exploit their abiding understanding of

---

[49] Joseph Votel, *Statement of General Joseph L. Votel, U.S. Army Commander Unites States Special Operations Command before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st Sess., 2015, https://docs.house.gov/meetings/AS/AS26/20150318/103157/HMTG-114-AS26-Wstate-VotelUSAJ-20150318.pdf.

[50] William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice* (New York: Presidio Press, 2009).

[51] NATO, *Allied Joint Doctrine for Special Operations*, AJP 3.5 (Brussels: NATO, 2013), https://standards.globalspec.com/std/1657612/AJP-3.5.

[52] Patrick Michael Duggan "Why Special Operations Forces in U.S. Cyber-Warfare?," *The Cyber Defense Review*, January 8, 2016.

> psychological, cultural, and societal factors that drive human behavior and for providing unrealized opportunities in persuasion and compulsion to shape the calculations, decision-making, and behavior of relevant actors. Adopting a discreet push-approach for cyberwarfare, SOF can channel the steady accumulation of small human and technical acts into an eventual psychological tipping point that changes the adversary's behavior.[53]

The phrase "gray zone," an oft-heard term in SOF and cyber literature, refers to the physical and virtual environment in time and space between deep peace (white) and deep war (black). Other frequently used synonyms are phase zero, pre-conflict phase, non-linear warfare, political warfare, deep-war, or left-of-the-launch. In recent years, various global incidents happened in this so-called gray zone. Russia is very active in this zone, as evidenced by the bloodless, but illegal, annexation of Crimea by initially unidentifiable and unbatched military, later known as "little green men." This activity provided under-the-radar support for the separatists in Donetsk. In addition, Russian activity in the gray zone has been implicated in the bloody civil war in Syria, and interference in America's elections. China and Iran are the other known hybrid-warfare participants, with a focus on cyber operations in the gray zone. China, in particular, uses very sophisticated online techniques to steal military intellectual property. As a result of this increased military action in the gray zone, Arquilla cited a need for doctrinal innovation in the United States.[54] That need was fulfilled by a Department of State Federal Advisory Committee, which defines the gray zone as "the use of techniques to achieve a nation's goals and frustrate those of its rivals by employing instruments of power—often asymmetric and ambiguous in character—that are not direct use of acknowledged regular military forces."[55] This is a complicated and confusing definition. Therefore, this thesis employs the term hybrid warfare or hybrid threat in its discussion about the integration of Dutch SOF and cyber means. "Hybrid threats combine conventional and unconventional, military and non-

---

[53] Duggan, "'Why Special Operations Forces in U.S. Cyber-Warfare?'"

[54] John Arquilla, "Perils of the Gray Zone: Paradigms Lost, Paradoxes Regained," *PRISM* 7 no.3, May 9, 2018.

[55] International Security Advisory Board, *Report on Gray Zone Conflict* (Washington, DC: U.S. Department of State, 2017), 1, https://2009-2017.state.gov/t/avc/isab/266650.htm.

military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives."[56]

The operational SOF environment and cyberspace share many similarities and differences. For instance, both involve covert or clandestine activities in a global and complex environment with different anonymous individual actors, groups, nation-states, or even transnational organizations.[57] The clandestine activities of SOF are comparable to stealthy cyber operations. The purpose of both is to assist in gaining political, economic, ideological, social, or religious dominance as well as a competitive advantage information position, by using global overt, covert, and clandestine operations.[58] Both have a relatively short preparation and recovery time, are relatively cheap, and have an opaque and stealthy character. The intent of SOF actions like DAs and SRs are similar to offensive cyber operations. Likewise, the intent of a MA operation could match the purpose of defensive cyber operations to strengthen a foreign state and thus safeguard its national political-military interests without a large-scale military involvement. It could also have a deterrent effect by serving as a warning of a country's capabilities.[59]

The most significant difference between SOF and cyber operations, however, is the high personal risk of the SOF operator in the field behind enemy lines, versus the relatively safe and secure desk jobs of the cyber experts in their home country or Forward Operating Base (FOB). Due to the use of the virtual domain, the cyber expert can operate from almost anywhere in the connected world, while the SOF operator needs to be physically in the area of operation near or at the target. Sometimes this means SOF are in conflict zones with poor infrastructure and living conditions. Alternatively, cyber combatants are not limited

---

[56] Frank Bekkers, Rick Meesen, and Deborah Lassche, *Hybrid Conflicts: The New Normal?* (The Hague: The Hague Centre for Strategic Studies and TNO, 2019), https://hcss.nl/report/hybrid-conflicts-new-normal.

[57] Sanchez, Lin, Korunka, "Applying Irregular Warfare Principles to Cyber Warfare," *Small Wars Journal* (1st quarter, 2019).

[58] Robert Koch and Gabi Rodosek, *ECCWS2016-Proceedings For the 15th European Conference on Cyber Warfare and Security* (Academic Conferences and Publishing Limited, 2016).

[59] Robert M. Gates, "Helping Others Defend Themselves," *Foreign Affairs*, June 2010, https://www.foreignaffairs.com/articles/2010-05-01/helping-others-defend-themselves.

by gender, physical conditions, or physical handicaps, whereas SOF personnel need to be physically fit, well trained, and always ready to operate in harsh conditions.

Given these differences and similarities, it is important for SOF and cyber operations to coordinate and cooperate. As stated by journalist Carlo Munoz in *The Washington Times*, "Pentagon and special operation command officials say the mission to fight extremist groups will remain a part of the special ops mandate, but that the command-level directives will place a larger premium on nontraditional skills in cyber and information operations."[60] That means that there is a growing demand for SOF and cyber capabilities to integrate and coordinate. During the Russian bloodless, yet illegal, annexation of Crimea in 2014, "Russian special operations teams used mercenary hackers."[61] These cyberwarfare proxies waged the online battle against Ukraine and prepared the area for the pro-Russian paramilitaries to successfully annex Crimea, effectively combining cyber effects with irregular (SOF) military operations. By using cyber-enabled special warfare primarily as a proxy, Russia was able to achieve important effects on the ground with minimal initial source attribution. This example shows that during the same operation, SOF and cyber capabilities could reinforce each other if they are properly integrated and synchronized. In some situations, it is perhaps no longer necessary for SOF to conduct a physical SR to prepare for a DA operation, while everything is already online prepared, documented, and exploited. Nevertheless, often insertions of malware into an enemy air-gapped network requires boots on the ground, usually those of SOF.

Cyber strategists Brandon Valeriano, Benjamin Jensen, and Ryan Maness stated that cyber operations rarely occur in isolation, usually interacting with other diplomatic and military means at the same time and in the same place.[62] The authors state that "cyber

---

[60] Carlos Munoz, "Special Ops Mission Shifts from Terrorism to China, Russia," *Washington Times*, February 24, 2019, https://www.washingtontimes.com/news/2019/feb/24/special-ops-mission-shifts-terrorism-china-russia/.

[61] Maurer, *Cyber Mercenaries*, 97–98.

[62] Brandon Valeriano, Benjamin M. Jensen, and Ryan C. Maness, *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford; New York: Oxford University Press, 2018), 90.

options are part of a larger campaign combined with other instruments."[63] To achieve specific ends in the information realm, military decision makers need a diverse, hybrid–threat–resistant toolbox, including SOF and cyber capabilities. With this filled cyber-SOF toolbox, there are opportunities in the information environment, including hybrid warfare. Here SOF can operate clandestinely below the threshold with cyber capabilities and with less direct accountability. Pavel Antonovish specifies this by writing, "Dividing lines between war and peace can be eroded conveniently in cyberspace. Damage (whatever its nature) can actually be done to an adversary without overstepping formally the line between war and peace."[64] Information and communications technology (ICT) exploitations, cyber-attacks, information operations (including influence operations), and SOF could play "significant roles in the cyber-enabled irregular campaigns in hybrid warfare."[65] To put this in context, Colonel Duggan explained this as, "Cyber-enabled special warfare could both deter conflict and be applied throughout the spectrum of conflict because it is well suited to all phases of operation, from shaping the environment through intense warfare through reconstruction."[66] At the end, the overall impression is that the integration of SOF and cyber operations could open a new world with many opportunities and possibilities. Cyber tools in combination with SOF allow a country to attribute and still remain in the shadows to mitigate the risk of escalation with adversaries.

C. SOF AND CYBER IN THE NETHERLANDS

Both Dutch SOF and cyber capabilities need more money to be effective and interoperable with NATO allies. The political unwillingness among several European states to provide higher financial NATO contributions has created tensions with the United

---

63 Valeriano, Jensen, and Maness, 23.

64 Pavel Antonovish, *International Conflicts in Cyberspace: Battlefield of the 21st Century* (U.S. Department of Defense, 2017), 57.

65 Duggan, "'Why Special Operations Forces in U.S. Cyber-Warfare?'"

66 Duggan.

States, possibly calling into question their future level of cooperation within NATO.[67] Even before President Trump's request in 2017 for European countries to boost their defense budgets, the Netherlands thought it took its responsibility seriously by increasing its MoD budget, which both SOF and cyber could benefit from.[68] However, the United States differs in this view. Recently, U.S. ambassador Pete Hoekstra announced that he was "not amused" with the slow progress the Dutch made to reach their 2% NATO defense goal.[69]

National doctrines dictate the modus operandi of the Dutch armed forces in cyberspace and in the SOF domain. If possible, national doctrines are aligned with, derived from, or substituted for allied doctrine. Should future allied doctrine describe military SOF and cyber operations as covered in this doctrine, NATO doctrine will necessarily have priority over national doctrine. Upon acceptance and publication of a NATO cyber or SOF doctrine, this national doctrine "will only be revised and issued for subjects not covered by that NATO doctrine, in cases where specific Dutch aspects need to be emphasized, or in cases where the Dutch vision differs from accepted NATO-vision, or even if clarification is required for the tactical level."[70] Until there is a national SOF doctrine, SOF operations for the Netherlands acts primarily under the umbrella of the NATO *Allied Joint Publication 3.5: Joint Doctrine for Special Operations*.[71] Therefore, the Netherlands, as a small state, use this NATO doctrine to define its SOF:

---

[67] Joyce P. Kaufman, "The U.S. Perspective on NATO under Trump: Lessons of the Past and Prospects for the Future," *International Affairs* 93, no. 2 (March 2017): 251–66, https://doi.org/10.1093/ia/iix009.

[68] Jorn Jonker and Niels Rigter, "Meer Geld voor Defensie" [More Money for Defense], *Telegraaf*, April 26, 2019, https://www.telegraaf.nl/nieuws/3503091/meer-geld-voor-defensie.

[69] Bastiaan Nagtegaal, "Amerikaanse Ambassadeur vindt Nederlandse Defensie-Investering te Weinig" [American Ambassador finds the Netherlands Defense Budget too Little], NRC, May 29, 2019, https://www.nrc.nl/nieuws/2019/05/29/amerikaanse-ambassadeur-vindt-nederlandse-defensie-investering-te-weinig-a3961999.

[70] Dutch Ministry of Defense, "The Netherlands Armed Forces Doctrine for Military Cyberspace Operations," 2.

[71] NATO, *Allied Joint Doctrine for Special Operations*.

> Military activities conducted by specially designated, organized, trained, and equipped forces using operational techniques and modes of employment not standard to conventional forces. These activities are conducted across the full range of military operations independently or in coordination with operations of conventional forces to achieve political, military, psychological and economic objectives.[72]

The demand for Dutch SOF capabilities is increasing. The post 9/11-period, with multiple Dutch military SOF deployments in Afghanistan, Iraq, Somalia, Mali, and other non-Western countries, enhanced the respect for special forces personnel. The expanded instability in Eastern Europe as a result of Russian hybrid actions, combined with the growing demand for national SOF taskings within the National Police,[73] even increased the demand for specially designated selected, trained, equipped, and organized Dutch military. Special Operations Forces with the Army SOF KCT (*Korps Commando Troepen*) and the Maritime SOF NLMARSOF (Netherlands Maritime Special Operations Forces) are the two available elite units in the Netherlands. Both units conduct operations under the wing of the newly established NLD SOCOM. Since December 2018, NLD SOCOM is growing into a mature command that will be fully operational in 2020. Increasing activities in hybrid warfare, both in the physical and the virtual environment, combined with more budget for the MoD, could accelerate the boost of Dutch SOF.[74] SOF, therefore, is currently "hot" and should use the opportunity and its momentum.

The Dutch MoD has recognized three types of military operations in the information domain, including operations with an offensive (active), defensive (passive), and exploitation (intelligence) nature.[75] All three options may create effects in cyberspace within and beyond the national Dutch systems and networks. According to the Dutch MoD doctrine, "Successful execution of military cyber operations requires an integrated,

---

[72] NATO.

[73] NLMARSOF has one squadron dedicated on stand-by for the national counterterrorism tasks within the National Police.

[74] Sander Zurhake, "Special Forces Worden Fundament voor Krijgsmacht" [Special Forces Become Fundament for Armed Forces], *De Groene Amsterdammer*, November 13, 2015, https://www.groene.nl/artikel/special-forces-worden-fundament-voor-krijgsmacht.

[75] Dutch MOD, "Nederlandse Defensie Doctrine," 2013.

synchronized, and comprehensive approach, underpinned by timely and effective intelligence preparation of the environment (IPE)."[76] Figure 1 shows the various phases of defensive and offensive operations from the Defense Cyber Command (DCC) within the cyber domain. The model differentiates between passive and active cyber operations and gives a clear line for when a mandate is necessary.

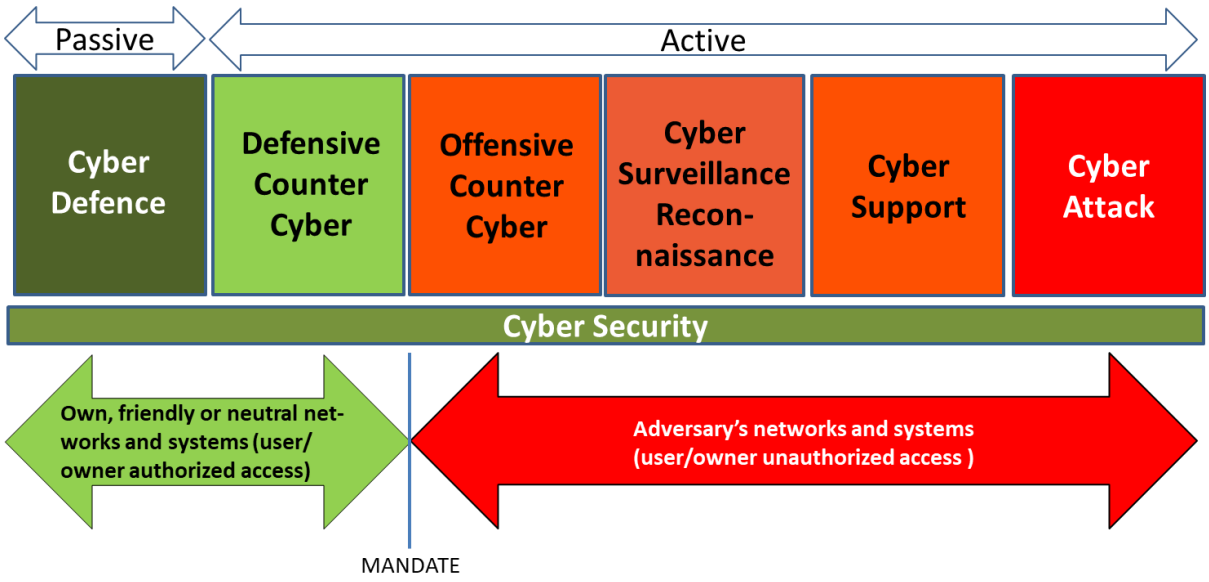

Figure 1. Dutch Military Cyberspace Operations and Activities[77]

The third approach, exploitation of intelligence operations in the cyber domain, is not shown in Figure 1, because this happens under the wings of the Military Intelligence and Security Service (MISS) and the General Intelligence and Security Service (GISS). Both intelligence services conduct their cyber operations under the umbrella of JSCU.[78] These activities are subject to the legal constraints within which the MISS and GISS operate and the scrutiny of the Intelligence and Security Services Supervisory Committee.

---

[76] Dutch Ministry of Defense, 22.

[77] Source: "The Netherlands Armed Forces Doctrine for Military Cyberspace Operations" Dutch MoD, 2019.

[78] Dutch MoD, 2019.

Next to strategic Cyber Intelligence, Surveillance, and Reconnaissance (ISR), the MoD uses operational and tactical Cyber ISR. Operational Cyber ISR focuses on the Commanders' operational needs (Commanders' Critical Information Requirement (CCIR)). Tactical Cyber ISR is relevant in supporting deployed or deploying units.[79] Nevertheless, cyber operations should easily manoeuvre vertically, from either the bottom-up from tactical, operational, and strategic, or the other direction, top-down.

Dutch SOF could operate under different circumstances for both DCC in a defensive and offensive role under a military mandate (Article 100 letter),[80] or via the *Ministeriële Kerngroep Speciale Operaties* (MKSO) procedure,[81] and for MISS in an intelligence exploitation role under the Intelligence and Security Act.[82] Dutch SOF can exploit, defend, and attack people, data, information, systems, and intelligence for national situational awareness, moral and social support in the physical and, eventually, in the virtual domain. Dutch SOF's future roles could be the shaping and preparation of the strategic context for the Netherlands to use its national instruments of power, including cyber capabilities. In this strategic context, "hybrid conflicts are the norm and human (SOF) behavior is the key."[83] In combination with cyber tools, the MoD, with the brand new SOCOM, has a filled toolbox to counter the hybrid threats in the current information domain, to support the Dutch and European comprehensive security approach.[84]

Nevertheless, the main question in this context is:

---

79 Dutch MoD, 2019.

80 Article 100 of the Dutch Constitution (decision-making process).

81 Dutch ministerial steering group committee for special operations with the prime minister, Foreign Affairs, and Defense ministers.

82 Wet op de Inlichtingen- en Veiligheidsdiensten 2017 [Law on Intelligence and Security Services], WIV, 2017.

83 Professor Martijn Kitze's speech, to the Special Operations Research Association, Monterey, CA, March 2019.

84 Markus Schmid, "The Concept of Comprehensive Security: A Distinctive Feature of a Shared Security Culture in Europe," accessed October 10, 2019, https://apps.dtic.mil/dtic/tr/fulltext/u2/a475775.pdf.

- How can Dutch SOF enhance the national cyber capabilities to counter the hybrid threats the Netherlands currently faces?

Therefore, this main question is the research question of this thesis. The next section explains the means to answer this question and by what methodology.

D. METHODOLOGY

To answer the key question of how to enhance Dutch SOF in the cyber domain against the hybrid threat the Netherlands currently faces, this thesis examines the relation of SOF and cyber operations in the military realm. It investigates the potential roles of SOF in the cyber domain and its possible integration, cooperation, synchronization, and coordination of capabilities on the strategic level, and how these affect the operational and tactical levels for the Netherlands. The thesis not only investigates the traditional SOF approach in the physical domain, but also searches for possible opportunities and gaps in the cyber domain—as the new fifth area in warfare.

Specifically, this thesis uses a qualitative heuristic methodology,[85] often used when making judgments about the probability of events under uncertainty, that solves problems by studying similar problems and discussing best practices. In this case, the Netherlands has various new military organizations (SOCOM and DCC) and is reorganizing its current MoD top-command structure. These organizational developments inside the MoD influence the SOF and cyber capabilities and will evolve in the future.

Therefore, this thesis examines the various aspects of NLD SOF by looking at their capabilities, then considers the ways they might, in general, have a role to play inside the cyber domain, and how SOF even possibly could integrate with the cyber domain. So, both SOF roles are examined in the context of the virtual and physical worlds.

---

[85] Gerhard Kleining and Harald Witt, "The Qualitative Heuristic Approach: A Methodology for Discovery in Psychology and the Social Sciences. Rediscovering the Method of Introspection as an Example," *Forum: Qualitative Social Research* 1, no. 1 (January 2000), https://doi.org/10.17169/fqs-1.1.1123.

The theoretical base for this is already laid down in the literature review,[86] with offensive, defensive, and exploitational intelligence approaches in the cyber domain. This review briefly described the basic principles, aspects, and dynamics of SOF and cyber operations, followed by the possible roles and capabilities in each other's domains. The thesis shows similarities, differences, strengths, weaknesses, and gaps in the roles of SOF and cyber capabilities for the Netherlands. The thesis also shows where SOF and cyber operators need to coordinate (including for deconfliction), cooperate, or separate their capabilities along their own different lines in current and future operations, and how the possible risks could be mitigated. The perspective, however, is always from that of the SOF and how SOF can enhance operations in the cyber domain.

Finally, the results of the research on SOF enhancing cyber capabilities are reviewed during interviews with Dutch SOF and cyber experts. The Netherlands is an example of a safe, regular, small European NATO state, which is now in transition to reorganize the top-command structure of the MoD, to include a newly formed SOCOM, DCC, and a growing SOF and intelligence community. As mentioned in the Chapter I, the Netherlands has to deal with hybrid threats. The discovered outcomes from the heuristic methodology will show the opportunities and possibilities on the strategic, operational, and tactical levels of hybrid conflict for the Dutch MoD. These outcomes are formed and directed by interviews with experts within the SOF (NLMARSOF and *Korps Commando Troepen*) and cyber (Fox-IT, MISS, and GISS) domains in the Netherlands, including commanders from the NLD SOCOM, Defense Cyber Command, and Joint SIGINT Cyber Unit, all of whom are based in The Hague. The interview questionnaire is enclosed as an appendix in this thesis and is processed and approved by the Institutional Review Board (IRB) of the Naval Postgraduate School.

The qualitative heuristic methodology is used in combination with the interviews to provide conclusions and recommendations about the possible roles for Dutch SOF in the cyber domain and the coordination, cooperation, or separation between the SOF and cyber capabilities, which the Dutch MoD hopefully could benefit from.

---

[86] Literature reviewed for this thesis is listed in the bibliography.

Given the hybrid threats the Netherlands is currently facing, the next chapter explains these threats in more detail, examines the Dutch counter cyber capabilities, assesses SOF's potential ability to fill the cyber gaps in the virtual domain, and looks at what role SOF could play to support operations in the cyber realm.

III. CYBER CHALLENGES AND SOF CAPABILITIES IN THE NETHERLANDS

> Today, small teams of special operators armed with asymmetric cyber-tools, irregular warfare tactics, and mass disinformation can have truly strategic effects.
>
> —General Joseph Votel,
> commander USSOCOM[87]

A. INTRODUCTION

Chapter III examines the current hybrid threats for the Netherlands and hypothesizes that there are insufficient Dutch cyber means to counter them. This chapter explains what capabilities are currently missing and how SOF can support cyber operations to fill these cyber gaps. By showing various unclassified examples, this chapter provides three potential ways Dutch SOF can support cyber operations to counter the hybrid threats the Netherlands currently faces.

B. DEFINING THE CURRENT HYBRID THREATS FOR THE NETHERLANDS

To answer the question of what the current hybrid threats for the Netherlands are, it is essential to understand what a hybrid threat is and what it means in a military context. As stated by the Dutch National Coordinator Security and Counterterrorism (NCTV), there is no universal definition.[88] Nevertheless, there are elements typically involved, like the integration of malicious actions via military forces (conventional and non-conventional), and non-military means conducted together. Threats arise when military exercises are too close to borders and intimidate neighbor countries, or there is the use of unidentifiable groups like special forces, proxies, private military organizations, and volunteers in

---

87 General Joseph L. Votel, USA, commander of U.S. Special Operations Command, email correspondence with Colonel Patrick Duggan, December 18, 2014.

88 National Coordinator for Security and Counterterrorism, *Χίμαιρα: An Analysis of the 'Hybrid Threat' Phenomenon* (The Hague: Ministry of Justice and Security, 2019), 9, https://english.nctv.nl/documents/publications/2019/09/05/analysis-of-the-'hybrid-threat'-phenomenon.

combination with diplomatic, economic, and informational (cyber) means to carry out semi-military operations. By using a mixture of DIME means,[89] state and non-state actors can influence, manipulate, disinform, and control. Moreover, these actors can sabotage, deter, deceive, and even attack the adversary and create a hybrid threat. To quote the NCTV: "The diversity of resources to be deployed is a requirement for being able to speak of hybrid conflict, because of the varied mix that is assumed." In this quote, the NCTV called it "conflict" instead of "threat" because conflict is a little more specific. As mentioned in the previous chapter, "hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives."[90]

The basis for the organization of Dutch society and prosperity is an open society with a market economy that focuses on freedoms, democracy, the rule of law, and international integration. Because of this openness, the Dutch benefit from the opportunities and possibilities that digital developments, globalization, and connectivity offer. As mentioned by the NCTV in an April 2019 letter to the Dutch Parliament about measures against state threats, "This open economy and free trade give the Netherlands necessary financing, economies of scale, exchange of languages, knowledge, and essential competitive incentives."[91] However, the downside for the Netherlands as an open, digitally accessible, and free society is the country's vulnerability to hybrid threats from state and non-state actors. These actors gain insights into decision making and try to influence politics via public opinion; "they enable digital sabotage of vital infrastructure, steal trade secrets, or intimidate and influence"[92] countrymen at home and settled abroad through diaspora. By using cyber-attacks, covert influence operations, and pressure via economic

---

[89] Diplomatic, Information, Military, and Economic means. The acronym is a useful reminder for military officers about the basic elements of national power.

[90] Bekkers, Meesen, and Lassche, *Hybrid Conflicts: The New Normal?*

[91] Ministerie van Justitie en Veiligheid, *Kamerbrief over Maatregelen tegen Statelijke Dreigingen* [Letter to Parliament about Measures against State Threats] - *Kamerstuk - Rijksoverheid.nl*, 2019, https://www.rijksoverheid.nl/documenten/kamerstukken/2019/04/18/tk-tegengaan-statelijke-dreigingen.

[92] Ministerie van Justitie en Veiligheid.

means, malicious actors can influence the political agenda. These political destabilization instruments are heavily intertwined with modern technology and create the environment for hybrid warfare and their threats.[93]

The current hybrid threats to the Netherlands are divided by the Ministry of Justice and Security into three groups: the digital threat, the economic security threat, and the threat of meddling by foreign state actors.[94] The first and most prominent group is the threat via digital means. New digital technologies, such as "blockchains, robotization, or artificial intelligence are rapidly transforming the economy and society."[95] Hidden vulnerabilities in commercial off-the-shelf (COTS) software retain value for possible future foreign military operations. Therefore, the GISS and MISS have advised the Dutch Parliament to avoid the Chinese Company Huawei to build a new 5G-network in the Netherlands.[96]

Digital transformation is the engine behind innovation and developments for the Netherlands. The downside, though, is the inherent national security risks, such as espionage, sabotage, disinformation, and strategic foreign dependencies. State actors like China, Iran, and Russia are using digital means to manipulate information, sabotage by disturbing vital processes, misinform by spreading false information via social media during elections, and conduct espionage for sensitive or confidential information.[97]

---

[93] Mark Galeotti, *Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right* (Online: Lulu Press, 2016).

[94] Ministerie van Justitie en Veiligheid, *Kamerbrief over Maatregelen tegen Statelijke Dreigingen - Kamerstuk* - [Letter to Parliament on Measures Against State Threats], http://www.rijksoverheid.nl.

[95] European Union, *Artificial Intelligence in Society* (Paris: OECD Publishing, 2019), https://ec.europa.eu/jrc/communities/sites/jrccties/files/eedfee77-en.pdf.

[96] Huib Modderkolk, "Kabinet Negeert Advies Inlichtingendiensten: Huawei niet geweerd bij aanleg 5G-netwerk" [Parlement Ignores Advise Intelligence Services: Huawei not banned during Construction 5G Network], *De Volkskrant*, July 1, 2019, https://www.volkskrant.nl/gs-b415e11d.

[97] NCTV Cyber Security picture Netherlands 2019 and cyber intelligence reports from the Military Intelligence and Security Service (MISS) and the General Intelligence and Security Service (GISS) warned for disinformation and espionage in the Netherlands.

Due to the high dependency on digital means, analogous alternatives and fallback options for the Netherlands are barely available, creating an even more significant threat during a malfunction or disruption of electricity supply and data communication.[98] Vital processes are highly dependent on these supplies and will quickly feel the impact of a malfunction. This became reasonably clear in June 2019, when a network failure at the Internet provider KPN resulted in a nationwide telecommunication disturbance and an unreachable emergency number for hours.[99]

The second hybrid threat is the one against Dutch economic security. Foreign acquisitions and investment in vital infrastructure or companies that develop high-quality technology can lead to an undesirable dependence on other states with a risk to the functioning economy. An example is the Chinese company Huawei, which is under consideration to install a proposed 5G network in the Netherlands.[100] The equipment of Huawei is used in one of the largest Dutch telecom provider networks, and potentially gives the Chinese government unique insight into Dutch customer data, including data belonging to the MoD.[101] Perhaps it is for this reason the city government of Amsterdam paused the current data-center boom in the Dutch capital, where the taxes are attractive and the electricity relatively inexpensive.[102] As a major city, Amsterdam with its numerous Internet nodes has the most data centers globally and needs first to formulate a policy and understand the economic security threat.

---

98 National Coordinator Terrorismebestrijding en Veiligheid, *Cybersecuritybeeld Nederland 2019* [National Coordinator for Security and Counterterrorism, Cyber Security picture Netherlands 2019, Cybersecurity Picture 2019], (The Hague: Ministerie van Justitie en Veiligheid, 2019), https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-online-tcm31-392768.pdf.

99 Floor Bouma "Noodnummer 112 urenlang niet bereikbaar door KPN-storing" [Emergency number 911 Unavailable for Hours due to KPN Malfunction], NRC, June 24, 2019 https://www.nrc.nl/nieuws/2019/06/24/noodnummers-niet-bereikbaar-door-landelijke-storing-kpn-a3964838.

100 Modderkolk, "Kabinet negeert advies inlichtingendiensten."

101 Modderkolk, *Het is Oorlog maar Niemand die het Ziet*, 239.

102 Bloomberg, "Too Much Information: Amsterdam Hits Pause on Data-Centre Boom," July 16, 2019.

The third threat is the meddling of foreign state actors inside the Netherlands, which usually is a slow process that in the longer term can lead to severe disruption and dysfunction of the democratic legal order and an open Dutch society. As mentioned by the NCTV report: "The integrity of political and administrative decision-making is only available through an independent judiciary, free and fair elections, and fundamental freedoms such as freedom of the press, academic freedom, and freedom of expression."[103] Therefore, during the general elections in 2017, Dutch authorities counted all the votes by hand to thwart possible Russian meddling and prevent the hacking of vulnerable election software. Interior Minister Ronald Plasterk said: "Now there are indications that Russians could be interested; for the following elections we must fall back on good old pen and paper."[104]

Apparently, the most significant hybrid threat for the Netherlands is via virtual means. Physical actions often outside the cyber domain support these virtual means. In addition to a simple digital attack resource, physical operations can also be deployed, usually by state actors, as shown by the Russian GRU attack on the OPCW building.[105] The spaces between the physical and virtual environments, which support each other, will shrink in the hybrid cyber threat the Netherlands currently faces.

Although it is often state actors who have the military and non-military capabilities to influence, deter, spy, sabotage, and attack critical Dutch infrastructure and organizations, non-state actors are increasing their ability as well, and are therefore used as proxy-instruments by states. Hacktivists, insurgents, terrorists, and jihadists have used the Internet

---

[103] Ministerie van Justitie en Veiligheid, *Kamerbrief over maatregelen tegen statelijke dreigingen - Kamerstuk - Rijksoverheid.nl*.

[104] "Dutch Will Count All Election Ballots by Hand to Thwart Hacking," *The Guardian*, February 2, 2017, https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking.

[105] See example in the introduction of this thesis.

for propaganda and fundraising for years.[106] Although these non-state actors themselves are not capable of initiating hybrid conflicts and threats, they can be used as proxies by state actors to influence, manipulate, or sabotage specific strategic foreign and security objectives.[107] Various examples already provided in this thesis showed that Russia is very effective at combining state and non-state actors to threaten other nations. It was Russian mercenary hackers, for example, who paralyzed the Estonian financial system in 2007.[108] Russian SOF paved the path via hackers and pro-Russian paramilitaries to the illegal annexation of Crimea in 2014.[109] And, in the United States, the Russian State-sponsored cyber hacker group Cozy Bear tried to steal information from various U.S. officials to influence the presidential election in 2016.[110] Moreover, in 2018 Russian military members in combination with cyber experts tried to hack the OPCW in The Hague.[111]

This implies both state and non-state actors are part of the cyber threats the Dutch are currently facing nationally and internationally. This intertwined relationship affects the internal and external security of the Netherlands. Therefore, there is no difference between national and international hybrid threats for the Netherlands in the cyber domain.

---

106 National Coordinator for Security and Counterterrorism *Cyber Security picture Netherlands 2019*, (The Hague: Ministry of Justice and Security, 2019), 15. Https://thehaguesecuritydelta.com/media/com_hsd/report/255/document/CSBN2019-EN-def-Web-01-tcm32-405804.pdf

107 National Coordinator for Security and Counterterrorism, *Χίμαιρα: An Analysis of the 'Hybrid Threat' Phenomenon*, 17.

108 Rain Ottis, "Analysis of the 2007 Cyber Attacks against Estonia," CCDCOE, accessed July 31, 2019, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

109 Maurer, *Cyber Mercenaries*, 97–98.

110 Joshua Eaton, "Report: Dutch Security Services Infiltrated Russian DNC Hackers," Think Progress, January 27, 2018. https://thinkprogress.org/dutch-cozy-bear-hack-957b8d72bfd0/.

111 "How the Dutch Foiled Russian 'Cyber-Attack' on OPCW."

C. ASSESSING THE DUTCH CYBER MEANS TO COUNTER THE HYBRID THREATS

The Netherlands has insufficient cyber means to counter the digital hybrid threats it faces. Too often new cyber scandals become public and expose the inadequacy of the Dutch cyber defense and the country's vulnerabilities.[112] Currently, the Netherlands employs two approaches to defend itself. First, there is the general approach, which is primarily focused internally on the Dutch defense system. Second, there is the specific approach, which is focused directly on the threatening actor itself. Both approaches are clarified in more detail in the following paragraphs.

The internally focused general approach explains the Netherlands' own physical material and non-material limitations and vulnerabilities, since this will be the first physical and virtual location where malicious actors will try to attack. By limiting foreign actors' intent on abusing the Dutch vulnerabilities through tighter security measures, the malicious impact will be reduced. Examples of this method of reduction are the emphasis on the responsibility of the analog redundancy of digital solutions in vital processes, to remove admissibility for information operations, to have a clear and consistent narrative with an integral governmental communication plan, and to further European Union (EU) integration with various commonly used tools, such as diplomacy, to increase the resilience to respond.[113]

The second approach has a more specific character and is focused directly on the external threatening actor itself. As noted, it is critical to know the enemy by learning from its strengths and weaknesses and to understand its goals, intentions, and moves. Predicting and identifying the possible routes the adversary will take gives the Netherlands the advantage of preparation, monitoring, and building bypasses in the system.[114] By using an

---

[112] Marissa van Loon, "Nog Eens Honderden Bedrijven Onbeveiligd Door Lek in VPN-Netwerk" [Once Again Hundreds of Companies Unsecure due to a Leak in the VPN Network], NRC-Handelsblad, September 29, 2019.

[113] National Coordinator for Security and Counterterrorism, *Χίμαιρα: An Analysis of the 'Hybrid Threat' Phenomenon*, 17.

[114] National Coordinator for Security and Counterterrorism, 33.

online bypass, it is possible to cut off the main route in the network, without sacrificing the Dutch own entrance to the "destination." By connecting the adversary's "dots," the Netherlands can link various events, see patterns, and draw conclusions in this specific approach to come up with sufficient counter measurements.

This second approach can be used not only in a defensive but also in an offensive way as shown in the summer of 2014. The Dutch Intelligence Services (GISS and MISS) were spying on the Russian state-sponsored cyber hacker group Cozy Bear. By conducting offensive cyber operations (OCO), the services gained access via security cameras. By using this second approach, the Netherlands watched Russian hackers break into U.S. email accounts from the Democratic National Committee, State Department, and even the White House. The Dutch exploited this intelligence and handed it over to the Federal Bureau of Investigations (FBI), which led to the first look into the Russian interference in the 2016 U.S. presidential elections.[115]

Nevertheless, both approaches are insufficient against the digital hybrid threat the Netherlands is currently facing. As mentioned in the Dutch Cyber Strategy 2018, "The increasing cyber threat requires a strong, international response based on international agreements."[116] The Dutch government wants to warn cyber-attacks perpetrators about their behavior publicly. This public warning requires first of all detection and then, political and possibly legal, attribution of the state-actor. Unfortunately, this is not happening enough yet, primarily because of the lack of detection and attribution instruments. In addition, when the actor behind a cyber operation (technical attribution) is found, it is not always clear for what state this actor is operating as a proxy. Unless the proxy is known, the Netherlands cannot deter an actor by confronting the country responsible in public, suggesting the Netherlands should rethink its attribution processes and instruments.

---

[115] Eaton, "Report: Dutch Security Services Infiltrated Russian DNC Hackers,.".

[116] National Coordinator for Security and Counterterrorism, *Cyber Security Assessment Netherlands* (The Hague: Ministry of Justice and Security, 2018), 7, https://english.nctv.nl/binaries/CSBN2018_EN_web_tcm32-346655.pdf.

Hence, the Netherlands has insufficient cyber means to counter hybrid threats either nationally or internationally. In general, the governmental agencies, including the MoD, have an inadequate level of knowledge about the use and possibilities of cyber in the military realm. Despite current developments to position cyber liaison officers,[117] the MoD still lacks management direction and a clear vision of how to integrate cyber in military operations. Senior decision makers miss the experience in the cyber domain and have a limited cyber awareness, which results in a flat view on command and control in the cyber realm. These decision makers' stovepipe thinking, traditional mindset, and lack of personal cyber experience result in biases, and the refusal to accept that those virtual circumstances have changed. Thinking only in the tactical, operational, or strategic stovepipe limits the scope for planners and decision makers. Statically doing what one has always been done without an open mind for change and innovation will setback cyber development. One can only make a joint combined cyber fist against the hybrid cyber threats by losing the stagnant mindset and thinking creatively and acting more broadly and with fewer boundaries among the various levels and organizations.[118]

Moreover, the personnel shortcomings like stovepipe thinking, traditional approaches, and lack of experience in the cyber domain, increase the insufficiency of the cyber means inside the MoD. For example, the MoD has inadequate career paths for cyber experts, and it lacks a cyber personnel policy.[119] Furthermore, the financial incentives are disproportionately distributed between MoD and civilian cyber organizations. In other words, a cyber expert can get much more money in the private sector, making it very difficult for the MoD to keep the most talented cyber experts onboard.

---

[117] Interviews with Commanders NLD SOCOM, DCC, JSCU, KCT, and NLMARSOF. All commanders agreed that the role of liaison officers between SOF and cyber is crucial. The Hague, September 9−11, 2019.

[118] Interviews with Commanders NLD SOCOM, DCC, JSCU, KCT, and NLMARSOF. All commanders agreed on a holistic inter-department view for SOF and cyber. The Hague, September 9−11, 2019.

[119] Interviews with Commanders Dutch DCC and JSCU. Both DCC and JSCU commanders agreed that recruiting and keeping the educated and experienced cyber personnel in-house is a real challenge. The Hague, September 10, 2019.

Overall, cyber illiteracy is the major cyber threat confronting the Netherlands today. As mentioned by co-founder and previous chief executive officer of the Dutch Internet technology company Fox-IT Ronald Prins, who is responsible for most of the encryption of the classified data for the Dutch Intelligence Services (MISS and GISS), NASA, NATO, and also seven of the biggest American banks,[120] "The biggest threat within cyber is the ignorance of the population itself."[121] This ignorance also applies to senior military decision-makers inside the MoD and creates cyber gaps and insufficient use of the available Dutch cyber means. This cyber ignorance results in stovepipe thinking of various military actors within the MoD, those who are not able to cooperate, combine, or integrate various ways and means outside their scope. In a governmental organization like the MoD, the person with the highest rank decides, while in technical civilian cyber organizations, the boss will listen to his cyber experts and use the specialists for decision-making.[122] Stovepipe thinking, stagnant mindset, and lack of experience will result in a fragmented operational design and prevent the MoD from gaining the full benefits of cyber operations. By lacking a broader joint military and inter-agency government approach, cyber operations miss opportunities to counter the hybrid threats the Netherlands faces.[123]

D. SOF'S POSSIBLE ROLES TO FILL THE CYBER GAPS

Dutch SOF can be used in three various roles to fill the cyber gaps by supporting cyber operations initiated by DCC and JSCU. Although SOF is certainly not the silver bullet for all cyber problems and gaps, and some roles are perhaps not useful in all (digital) operational environments, it should at least be considered in the planning of cyber operations. Dutch SOF characterizes itself (just like many NATO countries do) as a joint strategic asset that can "conduct special operations in uncertain, hostile, or politically sensitive environments to create effects that support the achievement of strategic-

120 Modderkolk, *Het is Oorlog maar Niemand die het Ziet*, 228.

121 Bustra, *Security Leaks for Sale*.

122 Modderkolk, *Het is Oorlog maar Niemand die het Ziet*, 39.

123 Interview with Commander JSCU, The Hague, September 9, 2019.

operational comprehensive objectives. These operations may be conducted using clandestine or covert capabilities/techniques and require mature and highly-trained operators."[124]

SOF's characteristics make them an effective and dynamic tool for cyber operations, enabling them to support cyber operations by "small-scale, clandestine, covert, or overt operations of an unorthodox and frequently high-risk nature, undertaken to achieve significant political or military objectives in support of foreign (cyber) policy."[125] Besides the joint nature of special operations with other conventional military means, Dutch SOF is also capable of working in a "combined and interagency setting by, with, or through indigenous or surrogate forces,"[126] including cyber.

Despite its military character, SOF is able to blend in with the local civilian environment by conducting overt, covert, or clandestine low-visibility operations (LVO) in hostile and even denied areas. This is where SOF distinguishes itself from human intelligence operators in extreme terrain and conditions. SOF is able to conduct operations for a long duration and has the endurance and persistence to operate independently from support and supplies in any climatological circumstances in the world.

There are three main reasons why SOF are a possible tool to support and execute cyber operations: 1) SOF can gain access to hard targets for cyber operations; 2) provide the means to get wetware, hardware, and software in or out the operation area; and 3) understand, deceive, and influence the cultural environment. Although these three reasons differ significantly, there could be an overlap among them—such as the possibility to establish one reason before conducting the following. They are not mutually exclusive; in other words, some conditions need to be in place first, before the next type of operation could start. For example, before a cyber technician can be extracted out of hostile environment (reason 2), SOF need first to understand, deceive, and maybe influence the

---

[124] NATO, *AJP 3.20 Allied Joint Doctrine for Cyberspace Operations*, Edition A, Version 1, 3rd Study Draft (Brussels: NATO, 2019), https://www.nato.int/cps/en/natohq/topics_78170.htm.

[125] Colin S. Gray, *Explorations in Strategy* (Westport, CT: Greenwood Press, 1996), 145.

[126] NATO, *AJP 3.20 Allied Joint Doctrine for Cyberspace Operations*.

cultural environment (reason 3) to set the right conditions for this extraction. Even so, each reason could be used as an umbrella for numerous kinds of SOF operations with various tactics, techniques, and procedures.

1. Gain Access to Hard Targets for Cyber Operations

Because of the digital environment of cyber operations, the planning, execution, and command and control could be theoretically orchestrated behind a desk from every connected platform (land, air, sea, or space) in the world. There are classified examples, however, where particular physical entries have to be created to conduct a virtual operation.[127] These cyber operations could not start without having physical boots on the ground to create points of entry and gain access to these so-called hard targets. These hard targets are often remote, isolated, and difficult-to-access physical objects, which are in this case interesting for the intelligence cyber community. SOF's character as an under-the-radar clandestine operating force, capable of blending in with the local habitat, and equipped with the proper reconnaissance, sabotage, breach, and fighting tools, make it a valuable initial entry force to support these cyber operations and set the conditions to break into computers, networks, and information systems in or around hard targets—or just to exploit tactical sites physically.[128]

Hacking into computers through active cyber operations (as depicted earlier in Figure 1) is often executed via an intrusion model. Figure 2 shows this intrusion model and the stages of this multifaceted process, which is distilled from the National Security Agency (NSA) director Rob Joyce's presentation during the Enigma 2016 conference.[129] The model is not technically or tactically focused, but could be used as an operational

---

[127] The author was told various first and second hand examples about classified operations where SOF was used as the initial entry force to pave the way for cyber operations.

[128] Tactical Sight Exploitation (TSE) is a task SOF normally conducts after clearing an area or building to search for fingerprints, signs, or (digital) evidence.

[129] Rob Joyce, *USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers*, YouTube, 0:35, January 28, 2016.

concept for intruders to reach their strategic objects in cyber operations.[130] Each stage (reconnaissance, initial exploitation, establishment of persistence, lateral moves, and collection-exfiltration-exploitation) in this model presents an opportunity to get deeper in someone's system to spy, influence, sabotage, collect, or even attack. Alternatively, this model shows in the defender's method, the measures necessary to counter or defend the cyber system.

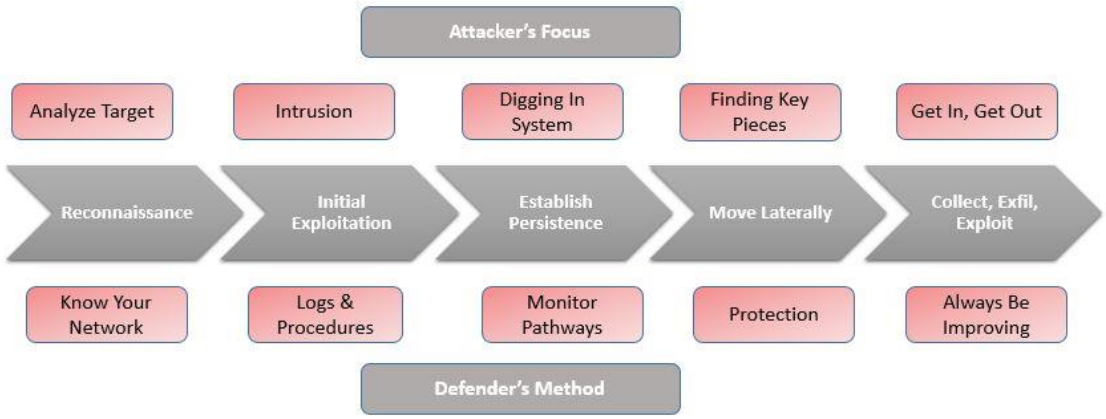

Figure 2. The Intrusion Model[131]

Especially in the first stages of the intrusion model, SOF's presence on the ground can be used as SR to collect information on the target (target acquisition) or be the initial entry force to bridge the gap between the physical and virtual environments (air gap). By this proximity, SOF could collect intelligence about the target and use radio-frequency technology to establish a connection with objects of interest, even when those objects are isolated from the Internet.[132] Then the cyber experts "back home" could exploit the gathered intelligence and could take over to focus on the next stage in the intrusion model.

---

[130] Buchanan, *The Cybersecurity Dilemma*, 33.

[131] "Cyber Security: Understanding the 5 Phases of Intrusion," *Graylog Blog*, accessed July 18, 2019, https://www.graylog.org/post/cyber-security-understanding-the-5-phases-of-intrusion.

[132] Classified documents provided by former NSA-employee Edward Snowden and seen by *New York Times* in 2013 prove this technique.

A good proof-of-concept is seen in U.S. government's formerly secret operation code-named "Olympic Games," better known as the Stuxnet attack.[133] During this combined NSA-CIA-Mossad operation discovered in 2010, an NSA-developed malware was delivered to an Iranian nuclear enrichment facility in Natanz to sabotage the centrifuges and stop the enrichment process. Although the enrichment facility was heavily protected and therefore not connected to a network, the CIA and Mossad used human assets to bridge the air gap and affect the Iranian system.[134] This shows that human assets, like intelligence operators, can collect intelligence and deliver digital malware like viruses, spyware, worms, Trojan horses, or ransomware without being physically connected to the Internet. In denied and hostile circumstances, in particular, SOF can be used as the human tool to resiliently bridge air gaps with technical equipment in various environments and climates during low visibility operations.

Another hypothetical example is the placement of technical devices to intercept, assemble, influence, disaggregate, disseminate, jam, or disturb data and systems in foreign countries. This device could covertly be placed by SOF close to the target of interest to intercept information for its assets.[135] This technique was probably also used in the Stuxnet example. According to *New York Times* journalists David Sanger and Thom Shanker, "What seemed to be an ordinary rock near a nuclear facility was in fact filled with electronic equipment that may have been relaying pilfered info or transmitting command and control instruction."[136] Sanger and Shanker continued, "In 2012, a unit of the Iranian Islamic Revolutionary Guards Corps moved a rock near the country's underground Fordo nuclear enrichment plant. The rock exploded and spewed broken circuit boards that the

---

[133] Alex Gibney, *Zero Days - YouTube*, 1:53:47, Documentary (Magnolia Pictures, 2016), https://www.youtube.com/watch?v=nnKdZyS3CKU.

[134] This human asset was recruited by the Dutch GISS after the request from the NSA and CIA. Huib Modderkolk, *"Het is oorlog maar niemand die het ziet,"* [It is War but Nobody Sees it] (Amsterdam: Uitgeverij Podium, September 2019).

[135] Buchanan, *The Cybersecurity Dilemma*, 34.

[136] David E. Sanger and Thom Shanker, "N.S.A. Devises Radio Pathway into Computers," *New York Times*, January 14, 2014, sec. U.S., https://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html.

Iranian news media described as the remains of a device capable of intercepting data from computers at the plant." [137] This example illustrated the potential for SOF and its imperative symbiotic relationship with cyber operations. SOF gain access to hard, difficult, and isolated physical targets by placing electronic or digital devices in extreme, rough, and dangerous terrain, which cyber can use for their online follow-on operations as the next step of the intrusion model.

2. Provide the Means to Get Wetware, Hardware, and Software in or out the Operation Area

SOF has various land, air, and maritime capabilities in its operational toolbox to get wetware, hardware, and software in or out of the operation area, highlighting another key role for SOF. In the land, air, and maritime domains, Dutch SOF is able to operate covertly via various ways and with a range of different mobility means. The air domain allows Dutch SOF the opportunity to use various rotary and fixed-wing options to drop off or pick up operators and their equipment, including parachuting through High-Altitude High-Opening and High-Altitude Low-Opening (HAHO/HALO), and conducting static-line jumps. In the land domain, SOF has various mobility means at its disposal, like quads, soft-tops, Bushmasters, armored vehicles, e-bikes, or any other vehicle that is needed.[138] In the maritime domain, SOF can conduct submarine-service operations in, under, and from the sea. By using boats, ships, frigates, submarines, water scooters, diver propulsion devices (DPD), or swim and dive capabilities, SOF can reach almost every location in the world from the sea.

Given these capabilities, Dutch SOF can function as an SR element, quick reaction force (QRF), counterterrorism (CT) unit, or force protector (FP) to support cyber operations. Moreover, with these capabilities, SOF is able to get wetware, including technical cyber experts or support agents, in and out of a hostile environment. Besides,

---

137 Sanger and Shanker.

138 *Factbook Korps Commandotroepen: Verleden - Heden - Toekomst* [Factbook Army SOF: Past - Current - Future], (Roosendaal, Netherlands: Koninklijke Landmacht, 2014), https://www.korpscommandotroepen.nl/wp-content/uploads/2015/01/Factbook-KCT-2014.pdf.

SOF can catch and arrest red-handed malicious hackers, hacktivists, cybercriminals, or cyber-terrorists, behind their computers or mobile devices. Subsequently SOF can extract such individuals, including their soft- and hardware, to hand it over to the local authorities. The confiscated hard- and software, gives the technical cyber, police, intelligence, and forensic experts immediate entry to the attackers' devices and proof for possible later prosecution and case building.

Furthermore, it is also possible to insert only soft- and hardware in a foreign country and infiltrate it in the area of interest, or give it to cyber experts who need it. This could be a USB stick or larger technical support equipment used to conduct a cyber operation successfully. Besides infiltration, it is also possible to exfiltrate important information devices and extract them to a safe location for further technical investigation. Both infiltration and exfiltration operations of soft- and hardware could be executed by SOF in all extreme environments and conditions in the air, land, and maritime domains.

As cyber expert Patrick Tucker notices, SOF could support cyber operations by "monitor [ing] and employ [ing] inconspicuous sensors and unmanned platforms to relay information across mobile deep learning devices equipped with 'neutral networks' capable of processing massive amounts of data, even classified, in someone's hand."[139] In the current information era, technically trained SOF operators could integrate Photo, Robo, Info, Nano, Geno, and Electro (FRINGE) technologies to bridge the cyber gap between the men and the machines.[140] All of these technologies are possible tools SOF could use in developments in the information environment like techno-social systems.

To clarify the use of FRINGE technologies to bridge the cyber gap between men and the machines, the Israeli raid in Syria is a good example. In July 2007, Israeli SOF conducted the preparations for the special operation mission code-named "Orchard" in the Syrian Desert. By bringing electronic warfare, cyber, and laser equipment inside Syria, the

---

[139] Patrick Tucker, "New Microchip Could Increase Military Intelligence Powers Exponentially," Defense One, February 4, 2016.

[140] Patrick Duggan "SOF's Cyber FRINGE" *Small Wars Journal*, July 19, 2019, https://smallwarsjournal.com/jrnl/art/sof%E2%80%99s-cyber-fringe.

Israeli *Shaldag* commandos were able to help electronic warfare and cyber warfare specialists set up a false-sky picture and jam the Syrian air defenses.[141] This deception operation enabled Israel to send F-15s and F-16s into the Syrian airspace, and to drop laser-guided bombs on the possible nuclear reactor site Al Kibar, without being detected by the radar station in Tall al-Abuad. As soon as the Israeli aircraft were in the vicinity of the Syrian site, the *Shaldag* commandos directed their lasers onto the reactor to guide the aircraft to their target. The nuclear reactor site in Al Kibar was completely destroyed.[142]

3. Understand, Deceive, and Influence the Cultural Environment

Lastly, according to Colonel Duggan and researcher Elizabeth Oren, SOF can support cyber operations by "providing keys to unlocking a deeper understanding of human interactions in cyberspace, and a means to contextualize the sociocultural, political, and historical factors which all too frequently fuel strife."[143] SOF's ability to blend in with the regional cultural environment, their often "unconventional operational and linguistic skills applied with adaptability, improvisation, innovation, and self-reliance,"[144] make them a small size unit with unique capabilities and self-sufficiency; SOF is the perfect tool to understand, deceive, and, if necessary, influence the cultural environment in foreign denied countries to pave the way for further cyber operations, without the immediate risk of further escalation.

---

[141] David E. Sanger and Mark Mazzetti, "Israel Struck Syrian Nuclear Project, Analysts Say," *New York Times*, October 14, 2007, sec. Washington, https://www.nytimes.com/2007/10/14/washington/14weapons.html.

[142] "The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor," *Der Spiegel*, accessed July 30, 2019, https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

[143] Patrick M. Duggan and Elizabeth Oren, "U.S. Special Operations Forces in Cyberspace," *The Cyber Defense Review* 1, no. 2 (2016): 73–80.

[144] "NATO - AJP-3.5

SOF can facilitate cyber operations by building relationships, establishing human networks, and creating local trust through key leader engagements.[145] By physically being in the theatre, SOF understands the local environment, recognizes future opportunities, and uses the vulnerabilities present to create entry points for possible cyber operations. SOF can draw the picture and set the conditions for the cyber experts in the initial stages of the intrusion model. Whether the human network of an adversary is using social media or other digital communications, it remains physical, and is therefore susceptible and vulnerable to cross-cultural interception and influences.[146] The strategic advisory goals can be manipulated, deceived, or influenced via physical or virtual entry points in the overlapping area between human and digital interaction. SOF can exploit both entry points with its own, cyber, or a combination of joint combined capabilities.

The prologue of this thesis gave a clear example of the overlapping area between human and digital interaction showing the Russian close-attack-hack—that is, hacking from a close distance to bridge the air gap—on the OPCW in The Hague, that clarifies the third reason for how SOF can support cyber operations. To prepare for the close-attack-hack, GRU intelligence cyber warfare operators blended in with the Dutch culture by posing as tourists in the Netherlands. As "tourists," they explored weak spots and thereafter used the Wi-Fi network as a physical vulnerable entry point to get inside the OPCW.

In another example, Russian SOF influenced the cultural environment to prepare for cyber operations, setting the conditions before the cyber-attack was launched to paralyze and annex Crimea. Using the pro-Russian population in Crimea to understand, deceive, and influence the Ukrainians, Russia gained all the advantage in an early stage of the hybrid conflict. By using pro-Russians as proxies in Crimea, Russian SOF were able to influence the regional culture and set the conditions for the next stage in the annexation of

---

[145] Jessica Turnley, *Cross-Cultural Competence and Small Groups: Why SOF Are the Way SOF Are*, JSOU Report 11–1 (MacDill Air Force Base, FL: The JSOU Press, 2011), 13, https://www.soc.mil/528th/PDFs/JSOU11-1turnleyF-DWDandSmallGroups(Turnley)_final(16Mar).pdf.

[146] Duggan and Oren, "U.S. Special Operations Forces in Cyberspace."

Crimea: a digital sabotage of three Ukrainian electricity distribution companies, which resulted in more than 200,000 consumers without power.[147]

Whether connected to the Internet or not, SOF could set the conditions directly or indirectly via proxies, allied partners, the indigenous population, and key leaders to take discrete human and technical actions and create entry points in the regional cultural environment. These physical and virtual entry points could be exploited by cyber experts back in the Netherlands to counter the current digital hybrid threats.

The three SOF supporting cyber-operations options explain the potential for how to fill the cyber gaps the Netherlands is currently facing. The three options show that it is plausible for SOF to support cyber operations by physically bridging cyber gaps. The next chapter investigates the integration options between SOF and cyber capabilities and what conditions and dynamics will influence their integration.

[147] Jackson School of International Studies, "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks."

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYZING THE INTEGRATION OF DUTCH SOF AND CYBER

> For too long, the Netherlands has been looking for a story about the available resources instead of the other way around.
>
> —Hirsh Balin,
> Scientific Council for Governmental Policy[148]

A. INTRODUCTION

This chapter assesses three viable options for the SOF-cyber integration to enhance SOF's ability to support these cyber operations. Previous chapters of this thesis demonstrated the strengths, weaknesses, and challenges in both the physical SOF and the virtual cyber terrain, and discussed the relationship between the two. This chapter focuses more closely on the actual integration of the physical SOF and the virtual cyber operations, and provides three viable options to accomplish this integration, including a short possible scenario in a vignette. The discussion also examines the challenges that will accompany this integration. Finally, this chapter describes how SOF and cyber can leverage their operations on the various tactical, operational, and strategic levels, and how these levels are connected and influence each other.

B. INTEGRATION OPTIONS FOR DUTCH SOF AND CYBER

Potentially there are many options to integrate SOF with cyber activities to support special cyber operations. This chapter, however, only examines the three most viable options, without comparing and weighting the options to present the most favorable. The viability of these three integration options is based on the heuristic methodology, with literature reviews, the examination of similar problems and their solutions in the United States, and interviews with SOF and cyber experts in the Netherlands.[149] The three options

---

[148] Department for Public Law, Jurisprudence and Legal History, *Veiligheid in een Wereld van Verbindingen: Een Strategische Visie op het Defensiebeleid.*

[149] The author of this thesis conducted various interviews in the Netherlands from September 9−11, 2019, with SOF and cyber specialists and pitched the cyber SOF integration options for viability.

are: 1) delegate cyber-SOF teams to the operational commands; 2) embed SOF and cyber personnel in each other's organizations; and 3) create a new cyber-enabled special operations unit.

1. Delegate Hybrid Cyber-SOF Teams to the Operational Commands

The Dutch MoD, with SOCOM in the coordinating role, in particular, could delegate the Army and Navy as the only two operational commands with SOF capabilities, to set up their hybrid cyber-SOF teams. This delegation could lead to cyber-SOF teams on the tactical and operational level, integrating with the SOF units of the Army and Navy, respectively, KCT and the Dutch Maritime Special Operations Forces. By doing this, SOCOM decentralizes the cyber-SOF teams and makes the operational commands responsible. Both operational commands have control over the hybrid cyber-SOF units, acting at the tactical and operational levels. Both KCT and NLMARSOF are tailored for their anticipated needs and according to their available resources and budget. These hybrid cyber-SOF teams could integrate into the traditional MA, SR, and DA taskings with cyber expertise. With this integration, SOF could provide better support to cyber operations on the tactical and operational levels.

The hybrid cyber-SOF teams would combine personnel with a technical cyber background and SOF experience, requiring deep specialization in both SOF operations and cyber techniques. The future operators in this team should know how to infiltrate into a denied or hostile environment, execute various SOF taskings, and at the same time code, encrypt, or manipulate social media by using advanced tools, such as FRINGE technologies.[150] The recruiting, training, and maintaining of these highly skilled and developed personnel will be challenging. Nonetheless, as mentioned by encryption manager Daniël Datau working for the Dutch encryption and software security firm FOX-It, "Sometimes you just have to start and see what challenges you will overcome and which

[150] Duggan, "SOF's Cyber FRINGE."

problems you have to solve."[151] By starting small both KCT and NLMARSOF could experiment with the SOF cyber integration on the tactical-operational level.

A scenario for both KCT and NLMARSOF on the tactical-operational level is the establishment of local decentralized cyber capabilities, which allows the Dutch SOF community to conduct bottom-up initiated SOF-cyber missions. If the proper mandate, legal framework, and infrastructure are in place, the tactical-operational cyber capabilities can achieve significant results. In military intelligence cyber operations, many things and techniques are already possible. These same standard techniques and capabilities could be used for offensive cyber operations. By investing only a few hundred thousand Euros, for buying imagery catchers, pineapple machines, and other simple digital interception devices, SOF should have sufficient infrastructure to start joint SOF cyber operations. With this in mind, however, a hacker should not become a SOF operator or vice versa. Therefore, it is sometimes easier to rent commercial personnel or put temporary cyber enablers in SOF teams, as explained in the second option.

a. Vignette for Integration Option 1

The Special Operations Maritime Task Group (SOMTG) Trident is fully operation capable at their maritime platform outside the exclusive economic zone somewhere off the coast of East Africa and waiting for further instructions from the Allied Maritime Command in Northwood, United Kingdom. When Trident receive their NATO-SOF mission set to infiltrate and collect intelligence on a local pirate network at one of the larger illegal camps near the beach, they start planning. Soon the SOMTG staff figures out that the only option to covertly insert personnel is by swimming or diving. All other options, with boats, helicopters, or even parachute drops, are too risky and could alert the security conscious pirates. SOMTG Trident has integrated technical cyber experts who are trained to swim and dive as well.

The next night, two buddy teams with one MARSOF operator and one technical cyber operator professional team are inserted from the Navy vessel with a small rubber

[151] Interview with encryption manager FOX-IT, Delft, September 10, 2019.

boat into the direction of the coastal pirate camp. The first team gets in the pitch-dark water, both connected with a snag line, and equipped with radios, weapons, and technical cyber equipment. After 20 minutes, the boat driver receives a call that the first team missed their target due to the strong current. The second team is inserted from a different angle and, within two hours, they manage to swim to the beach and infiltrate into the hostile pirate camp. Here they covertly install a technical interception device that makes it possible to intercept and decrypt all local radio traffic, including the encrypted signals used for their mothership to enter commercial vessels. With this information, SOMTG Trident is able to track and intercept all messages, which leads to the arrest of many pirates who were caught in action outside the East African country's territorial waters.

2. Embed SOF and Cyber Personnel

Integration option 2 is to embed SOF personnel in cyber organizations or vice versa, which is already happening on the staff level. On the strategic level, SOCOM has a cyber officer liaising with DCC and JSCU.[152] On the operational and tactical levels, both KCT and NLMARSOF have cyber liaisons in staff positions as well. Yet, there are almost no SOF planners or even operators working in the DCC or JSCU. In turn, no cyber experts or operators are working in the SOCOM, KCT, or NLMARSOF, except the liaisons.

Embedding specialized personnel in each other's organizations will benefit the cultural understanding and situational awareness of both SOF and cyber personnel, and bridge the cultural gaps. Doing so is complicated as well, however, because of the cultural institutional differences and backgrounds. Mutual understanding and respect will demand an extended commitment from both cyber and SOF personnel and their organizations and leadership. The specialists need to train, exercise, and educate one another to learn the tactics, techniques, and procedures of SOF and cyber operations. As soon as there is a basic understanding, SOF and cyber personnel could embed in task-organized teams, which fit future taskings. A flexible mentality is vital because every mission demands a different approach to supporting cyber operations. Sometimes SOF personnel will only support

[152] Interviews with Commanders NLD SOCOM and Dutch DCC, The Hague, September 9−10, 2019.

cyber operations by being physically in a holding area, ready to act as a quick reaction force, and occasionally cyber experts are embedded in a SOF team while they are inserted into or extracted out of the operation area. Both ways of embedding personnel, though, demand training, time, and patience in order to bridge the cultural gaps, and enable personnel to understand one another.

To sketch a scenario, both SOF and cyber personnel could start with an internship within each other's organizations to learn and understand the culture, techniques, procedures, and the planning processes used by their respective groups. By embedding personnel in each other's organizations, the foundation will be laid down for fruitful coordination, cooperation, and finally, integration. Due to the scarcity of technical cyber personnel, the MoD has started a project with reserve cyber experts.[153] Both the SOF and cyber organizations could use this pool of cyber experts when they are planning for operations requesting specialized cyber techniques, coding, or encryption.

a. Vignette for Integration Option 2

After accomplishing their first NATO-SOF mission in the African pirate camp, SOMTG Trident receives new orders from Northwood to physically install malware on a secure server in a medium regional city. The purpose is to intercept the pirates' email traffic, which hopefully can give NATO a better understanding of the financial networks that the pirates use. The cyber experts have already flown in and are waiting as tourists in a hotel in the city. They need their interception equipment, which they could not bring in via commercial flights. SOMTG Trident should provide a screen during the interception operation, and in case of emergency, react as a QRF to protect and, in worst case, extract the cyber experts back to the maritime platform.

Due to the long and intensive joint education, training, and exercises in their home country, the SOF and cyber teams know each other very well. They speak the same language and understand each other's tactics, techniques, and procedures (TTP), which leads to a smooth link-up and handover procedure at the hotel with the SOMTG's LVO

[153] Interview with Commander Dutch DCC, The Hague, September 10, 2019.

team. During the actual close target hack at the data center, the LVO team provides a covert screen, which would act as an early warning system and alert the cyber team in case of a possible compromise. As soon as the hack is accomplished, the cyber team returns to the hotel, and the LVO team exfiltrates via the water back to the maritime platform, safe and secure beyond the horizon. The malware is successfully installed and the surveillance begins.

3. Create a New Cyber-enabled Special Operations Unit

The third integration option to enhance SOF supporting cyber operations is to create a new centralized cyber-enabled special operations unit that operates directly under the strategic wings of SOCOM or DCC/JSCU. Under these wings, such a unit could "serve as the single authority to plan, coordinate, and build for global cyber-SOF operations."[154] From this strategic level, both the Army with KCT and the Navy-Marine Corps with NLMARSOF could benefit from this cyber-enabled special operations unit by embedding these teams during exercises, training, and ultimately operations. By having strategic cyber-enabled special operation teams, SOF can support cyber operations to 1) gain access to hard targets for cyber operations; 2) provide the means to get wetware, hardware, and software in or out the operation area; and 3) understand, deceive, and influence the cultural environment.

This cyber-enabled special operations unit would need a staff element to plan, control, liaise, develop, sustain, and build the new group. Depending on the main effort and legal framework for an operation, this staff element could act as a sub-unified command under the wings of SOCOM or DCC/JSCU in a supported or supporting role. This dual-headed orientation would give the staff flexibility and creativity.[155] A mission set under the umbrella of a cyber-oriented command, such as DCC and JSCU, demands

---

[154] Benjamin Brown, "Expanding the Menu: The Case for CYBERSOC," *Small Wars Journal*, June 7, 2018, https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc.

[155] In interviews with Commanders NLD SOCOM and Dutch DCC, both commanders stressed the importance of a flexible and creative mindset within SOF-cyber operations, where the command relationship is supporting or supported. The Hague, September 9−10, 2019.

more technical expertise than one under SOCOM where a more tactical approach is needed. Ultimately, the legal framework decides what kind of techniques and types of cyber operations are allowed.

To picture a scenario, this cyber-enabled special operations unit could divide its focus and expertise among special warfare such as MA and Special SR and surgical strikes like DA. In special warfare, the cyber-enabled special operations unit places more emphasis on the regional background and lingual skills, to improve the blending in the local environment. Although there is still a need to understand coding, encrypting, and the use of earlier mentioned FRINGE technologies, the focus in special warfare is more on the cultural climate. That is, the emphasis is on understanding the local habitat with its own habits, routines, customs, and population. Therefore, special warfare has more similarities with the third option of SOF's support opportunities: understand, deceive, and influence the cultural environment. As mentioned by the information systems and security professional Benjamin Brown in *Small Wars Journal,* "these [cyber enabled special warfare] teams would conduct indirect, less-technical activities in cyberspace, such as social media initiatives or cyber capacity-building, and often do so in cooperation with partner governments or groups."[156]

Within surgical strike scenarios like direct actions, cyber-enabled special operators should focus more on cyber techniques. These operators should be highly skilled in systems and computer science, understand FRINGE technologies and their functions within the denied or sensitive cyber domain. As Brown mentioned in his article, "These [cyber enabled surgical strike] teams would perform more direct and often unilateral cyber special operations, such as crippling adversaries' command and control (C2) systems launching cyber-attacks to disable target defense installations or infrastructural facilities."[157] By understanding the dynamics of MA, SR, and DA operations, the cyber-enabled special operation teams could be used in the whole spectrum of SOF operations and provide support to further cyber operations.

---

[156] Brown, "Expanding the Menu: The Case for CYBERSOC," 6.

[157] Brown, 6.

a. Vignette for Integration Option 3

The installed malware at the African data center was discovered by the local authorities and the whole data center was temporally disconnected. The Navy vessel with SOMTG Trident is not in the vicinity anymore. This left Northwood dark with no situational understanding of the pirates' financial flows. The next opportunity for NATO is the MA exercise with the African partnership. Army SOF has been training already for years with their African partners and has built a reliable network with local key leaders among politicians, military, police, and Islamic clerics to create regional cultural awareness.

During the Army SOF-led MA exercise, a cyber-enabled special operations unit from the strategic level has blended in to learn from their Army SOF colleagues' cultural awareness. After a couple of weeks, under the umbrella of the MA training and with the help of the local trusted key leaders, they undertake a covert cyber campaign against the pirates in their illegal coastal camps. With local knowledge, the cyber-enabled special operations unit knows how to target the pirates digitally, launch social media campaigns by using the pirates' identity to blackmail, manipulate, and deceive the pirate leaders. This results in more chaos and instability among the pirates, which the local authorities could benefit from and a gives NATO better situational understanding.

C. DYNAMICS AND CONDITIONS CHALLENGING THE SOF CYBER INTEGRATION

This section explains the dynamics and conditions that could challenge and influence the SOF and cyber integration. It is not the intent of this section to compare the three integration options for SOF to support cyber operations and draw conclusions. This comparison could be a separate thesis with various qualitative data, selection, and research criteria—all critical for and defined by the Dutch MoD. Nevertheless, it is important to understand the dynamics and conditions affecting both the SOF and cyber organizations and influencing the three integration options of 1) delegating cyber-SOF teams to the operational commands, 2) embedding SOF and cyber personnel within each other's organizations, and 3) creating a new cyber-enabled special operations unit.

In all three integration options, legal framework, finance, culture, command and control, and coordination are some of the critical conditions needed for the viability of each approach. These conditions are not all-encompassing and, depending on the environment and political circumstances, the list could grow longer. There are, however, three critical considerations for assessing the viability of the three integration options: mission impact, feasibility, and the mitigation of possible risks.

The first consideration is mission impact, defined as the efficiency and effectiveness of each integration option, in meeting the goal of enhancing the national cyber capabilities. Functional SOF and cyber teams are more independent of each other, whereas horizontal project teams have a very high level of interdependence. To increase their effectiveness, the horizontal SOF and cyber units need an aligned relationship between interdependence, as an aspect of complexity, and the appropriate means or mechanisms for coordinating the workflows, such as the rules, hierarchy, supervision, and mutual adjustment and horizontal communication.[158] Having these two entities with various backgrounds, types of education, and perhaps even viewpoints, requires an integration option with the best deconfliction, coordination, and synchronization.

The second condition that will influence the integration option is based on feasibility, which requires setting up decisive principles for success. By examining the integration, deconfliction, coordination, and synchronization of each option, the success of the combination can be measured. It is relevant to keep the dynamics and conditions in review, however, because they will affect and influence all three integration options. For example, the legal framework will decide whether this is an intelligence exploitation operation under the umbrella of the security intelligence services such as the MISS and GISS with the JSCU, a *Ministeriële Kerngoep Speciale Operaties* (MKSO) procedure, or an Article 100 letter operation under the direction of SOCOM or DCC. All frameworks request different juridical approaches to legitimize the type of operations.

---

158 Richard L. Daft, Jonathan Murphy, and Hugh Willmott, *Organization Theory and Design* (Mason, OH: Cengage Learning EMEA, 2014), 277.

Another dynamic that influences a feasible integration is the cultural aspect, because SOF and cyber personnel have different backgrounds. It will be a challenge to get technical cyber experts and tactical SOF operators under the same roof.[159] Cultivating excellent leadership is necessary to understand what either capability can accomplish. "Planning and thinking innovatively about how the capabilities contributed to cyber and special operations campaigns for strategic effects are essential"[160] for bridging the cultural gaps. Moreover, command, control, and coordination should be very well in balance between the two entities. If the choice of integration will be a centralized, decentralized, or pooled-divisionalized structure, the feasibility assessment should also take notice of the barriers and resistance versus the facilitators and drivers in the actual cultures and how reciprocal the cyber and SOF activities are.[161]

The third critical consideration is risk mitigation involved in the integration of SOF and cyber operations. Lessons from the past show that the operational commands, in particular, tend to operate in a stove-piped manner. Both KCT and NLMARSOF follow their training pipelines with particular recruiting, selection, and training criteria.[162] This stovepipe approach resulted, for example, in different end-states between the Army and Navy about similar training courses like sniper, CT, jungle, mountain, and arctic warfare. Decentralizing and delegating could be inefficient, especially for cyber capabilities. Fortunately, in recent years, the Chief of Defense (CHOD) of the Netherlands gave more direct guidance to the operational commands and established joint organization components. Nevertheless, the risk of stovepipe thinking within the operational commands still requires strategic guidance and integration cooperation from the MoD department. To

---

159 In interviews with Commanders NLD SOCOM and Dutch DCC, both the SOCOM and the DCC commanders mentioned that culture and mutual understanding between SOF and cyber personnel is the primary focus for a correct integration. The Hague, September 9−10, 2019.

160 Brown, "Expanding the Menu: The Case for CYBERSOC."

161 James D. Thompson, *Organizations in Action: Social Science Bases of Administrative Theory*, 7th ed. (New Brunswick, NJ: Transaction Publishers, 2003).

162 Conference call with Commander NLMARSOF; Commander NLMARSOF has no issues with having own NLMARSOF courses. However, cyber needs to be coordinated from the strategic level for both NLMARSOF and KCT. Monterey, September 26, 2019.

exploit cyber-warfare operations and gain the most significant effect, cyber and SOF personnel, including their capabilities, need a central structure under the wing of SOCOM, DCC, or JSCU depending on the type of operations. The United States, in its USSOCOM and USCYBERCOM, is currently struggling with the same dynamics. Their mitigation approach is to build a Cyber Special Operation Command (CSOC),[163] as per the third option in this chapter.

Other risks that should be mitigated are the lack of reciprocal awareness and understanding resulting from cultural differences between SOF and cyber personnel, including their professional SOF and cyber jargon, and technical versus tactical expertise. SOF and cyber staff personnel use various planning cycles, such as the cyber kill-chain and the intrusion model versus the special decision-making process (SDMP). Maybe the most important risk to overcome is the biases before the integration. Winning the hearts and minds of all the involved personnel in the reorganization is essential for a successful integration.[164]

MoD and its stakeholders should investigate all the pros and cons of the three viable integration options. Depending on the level of the organization (strategic, operational, or tactical), its structure (centralized, decentralized, or pooled-divisionalized), and the influence of the three considerations (mission impact, feasibility, and the mitigation of possible risks), MoD should bring the various stakeholders from SOF and cyber around the table to start brainstorming, compare the options, and examine the effects that would be achieved within the SOF and cyber operations.

On the other hand, if the MoD decides to integrate SOF and cyber and use one of the mentioned integration options, or a combination of these, it will require time, effort, and resources. The MoD should start with talent acquisition to select personnel and train both cyber-craft and SOF specialized tactics, techniques, and procedures. As cyber expert Benjamin Brown mentioned: “Innovative recruitment and training pipelines are crucial to

---

[163] Brown, “Expanding the Menu: The Case for CYBERSOC,” 7.

[164] Interview with Commander Dutch DCC Commodore Boekholt O’Sullivan, The Hague, September 10, 2019.

attract and prepare these new cyber operators."[165] The MoD should get skilled personnel from the private or academic sectors, who are physically fit and can parallel SOF and cyber techniques. These cyber operators should conduct sufficient training, exercises, and ultimately operations together with SOF. This integration demands a direct, centralized command and control that can mitigate the risks, build relations among SOCOM, DCC, MISS/GISS, JSCU, and operational commands. The staff should liaise with other departments in the Dutch government, civilian partners, and EU and NATO allies to keep each other informed, promote deconfliction, and the communication going.

D. SOF AND CYBER PLANNING ON VARIOUS LEVELS

Both SOF and cyber operations have an intertwined bond and show a symbiotic relationship on strategic, operational, and tactical levels, but their planning differs. SOF and cyber operations are both developed, planned, and decided for at the strategic level. The execution of operations, however, is often at the tactical level. In turn, this tactical execution has effects on the operational and strategic levels.

The MoD has an authentic and universal top-down approach in its planning. The strategic level gives planning guidance and establishes the required effects that need to be achieved. Next, the operational commands, including SOCOM and DCC, will start developing plans and missions for their sub-units on the operational and tactical level.

SOCOM uses this top-down approach as well to give the operational commands direction and guidance for both KCT and NLMARSOF in the planning of SOF operations. However, the practice in the real world often looks different, not always with this top-down structure. The SOF bottom-up approach is therefore an exception in the military realm. Often SOF seek out loopholes to conduct operations, which is still in line with strategic intent, but is mostly self-inflicted and executed.

[165] Brown, "Expanding the Menu: The Case for CYBERSOC."

Cyber, on the other hand, also has a different approach, which uses more of a spiral planning cycle to keep up with fast-moving technology and developments.[166] Spiral planning uses, for example, the intrusion model (see Figure 2, earlier in this thesis), and can accelerate or delay progress between the various steps of the planning process. Spiral planning enables cyber planners to introduce new commercial products more quickly and better prepare them for evolving threats.[167] Although a cyber exploit can be very useful today, it can be worth nothing tomorrow due to the adversary digital counter measures. Despite the strategic authority to plan cyber, and considering the proposed effects, including government decisions, mandates, and rules of engagement (ROE), lots of the autonomous cyber planning and execution happens on the operational and tactical levels.[168]

The use of cyber capabilities can be earmarked, just like SOF, as a special operation, which needs approval from the ministerial steering group committee of special operations.[169] Recently the procedure for the ministerial steering group committee on special operations was adjusted to involve offensive cyber operations executed by the DCC,[170] prior to the actual planning.[171] Hence, both SOF and cyber operations can be

---

166 Interviews with cyber expert Jelle Haaster and FOX-IT encryption manager Daniel Datau. Both explained the differences between the conventional SOF planning versus the spiral cyber planning. The Hague, September 10−11, 2019.

167 Amber Corrin, "Navy: Faster Acquisition Key to Cyber Defense," FCW, June 28, 2011. https://fcw.com/articles/2011/06/28/cyber-warfare-summit-acquisition-reform-strategies.aspx.

168 Dutch Ministry of Defense, "The Netherlands Armed Forces Doctrine for Military Cyberspace Operations," 2019.

169 A.Th.B. Bijleveld-Schouten, "Vaststelling van de begrotingsstaten van het Ministerie van Defensie voor het jaar 2018 ; Brief regering; Reactie op verzoek commissie om inzicht in besluitvormings- en verantwoordingsproces inzake speciale en geheime operaties," officiële publicatie, Staten-Generaal der Tweede Kamer, [Determination of the Ministry of Defense Budget Statements for the year 2018; Government letter; Response to Committee's Request for Insight into Decision-Making and Accountability Process regarding Special and Secret Operations, Official publication States General of the Second Chamber], March 27, 2018, https://zoek.officielebekendmakingen.nl/kst-34775-X-88.html.

170 Interview with Commander Dutch DCC Commodore Boekholt O'Sullivan, The Hague, September 10, 2019.

171 BG Paul Ducheine and LTC Kraesten Arnold,"Besluitvorming Bij Cyberoperaties," [Cyber-Operations Decision-Making] *Militaire Spectator*, accessed August 12, 2019, https://www.militairespectator.nl/thema/recht-cyberoperations/artikel/besluitvorming-bij-cyberoperaties.

triggered, planned, and executed on every level. They only need approval from the strategic stage because of the possible political and diplomatic consequences, impacts, and effects they could generate.

However, the first quick win for the MoD with SOCOM and the operational commands, in particular, is the integration of SOF and cyber experts and their capabilities in the planning process. As mentioned during the interview with Commander SOCOM Major General ten Haaf, "When we are looking at SOF and cyber operations, we should consider the whole process from the starting point to the end of the operation, when the evaluation is finished. Currently, we see that cyber is integrated too late into the planning process."[172] This SOF cyber integration means also learning from each other. Commander DCC Commodore Boekholt O'Sullivan described it during the thesis interview as follows: "SOCOM is short-term focused, while DCC is more oriented on a longer period. SOF personnel needs to slow down in their decision-making versus DCC who could learn to accelerate in their process or at least explain to SOF to slow down."[173]

This chapter showed three integration options for SOF and cyber operations. It provided the MoD several potential ways to successfully integrate SOF and cyber operations. The conditions and dynamics demonstrate that there are many variables that will influence effective and efficient integration. This chapter also revealed the symbiotic relationship both SOF and cyber display in the tactical, operational, and strategic theatres.

The next and final chapter of this thesis presents conclusions and offers useful and constructive recommendations for MoD staff and senior military decision makers in the SOF and cyber branches. Finally, it gives suggestions for future C-SOCC and NATO cyber SOF integration, including areas for further inquiry and research.

---

[172] Interview with Commander NLD SOCOM, The Hague, September 9, 2019.

[173] Interview with Commander Defensive Cyber Command, The Hague, September 10, 2019.

V. CONCLUSION AND RECOMMENDATIONS

> If you want to make beautiful music, you must play the black and the white notes together.
>
> —President Richard Nixon[174]

A. INTRODUCTION

This thesis has envisioned how Dutch SOF could support cyber operations to counterbalance the hybrid threat the Netherlands is currently facing. The thesis research has used a heuristic methodology, a review of the relevant literature, and interviews with Dutch cyber and SOF experts, including the commanders of the Special Operations Command, Defense Cyber Command, Joint SIGINT Cyber Unit, and both operational Dutch SOF units *Korps Commando Troepen* (KCT), and the Maritime Special Operations Forces. The research offers three SOF options to support cyber operations and examines the three viable integration probabilities.

This thesis has aimed to investigate the imperative symbiotic relationship between SOF and cyber capabilities within the military national instrument of power at the strategic level and its impact on operational and tactical levels of the hybrid conflict. The thesis is limited in scoped by the approach of viewing only the roles SOF could play to support cyber operations and not the other way around. The purpose is to give the Ministry of Defense with SOCOM, DCC, and the Dutch SOF in particular, handles for further cooperation, coordination, deconfliction, and ultimately, the integration of more efficient and effective SOF and cyber capabilities to make a combined fist against the hybrid threat the Netherlands is confronting.

---

174 Richard Nixon, "The Quotable Richard Nixon," Richard Nixon Foundation, April 25, 2011, https://www.nixonfoundation.org/2011/04/the-quotable-richard-nixon/.

B. SUMMARY OF FINDINGS

By providing the MoD with three roles in which SOF could support cyber operations, followed by three integration options including the challenges, conditions, and dynamics that will influence the integration, this thesis gives an answer to the main question:

- How can Dutch Special Operations Forces enhance national cyber capabilities to counter the hybrid threats the Netherlands currently faces?

The three possible roles for SOF to support cyber operations are: 1) SOF can gain access to hard targets for cyber operations; 2) SOF can provide the means to get wetware, hardware, and software in or out of the operation area; and 3) SOF can understand, deceive, and influence the cultural environment. Although these three roles differ significantly, there could be an overlap among them. Nevertheless, SOF is not the silver bullet for supporting cyber operations. There are many options in the cyber toolbox to deal with the hybrid threat, and these three SOF options are therefore just one tool for the Dutch cyber organizations.

The three integration options for SOF, including cyber capabilities and personnel, are for SOF and cyber organizations: 1) to delegate personnel into cyber-SOF teams to the operational commands; 2) to embed SOF and cyber personnel in each other's organizations; and 3) to create a new cyber-enabled special operations unit. This thesis did not compare or prefer any of the options. Although every integration option has advantages and disadvantages, it is important to take all the considerations that are important for the MoD and its stakeholders and see what effects are intended on the various levels (tactical, operational, and strategic). Conditions such as legal framework, finance, culture, command and control, and coordination are critical to consider in determining the viability of integration. Furthermore, depending on the environment and political circumstances, such conditions will finally determine whether the integration is successful. For assessing the options, there are three critical considerations: mission impact, feasibility, and the mitigation of possible risks.

C. RECOMMENDATIONS

During the literature review, talks with U.S. SOF and cyber colleagues, students and professors at the Naval Postgraduate School, and interviews in the Netherlands, it became clear that all three potential SOF roles supporting cyber operations depend on effects, conditions, and end states of the MoD. Integration, on the other hand, requires understanding of the strengths, weaknesses, and cultural gaps between SOF and cyber personnel and their organizations.

To use the full potential of the available Dutch cyber capabilities, the existing weaknesses must be reduced. The strength of cyber capabilities is that, when connected with the Internet, the physical location of those capabilities does not matter, which provides the means to stay under the radar with minimal risk for escalation. Cyber capabilities rapidly implement new ideas and technologies. By contrast, the shortcomings of the cyber domain are the slow pace of decision-making process; zero days are costly and very time consuming, can only be used once, and can backfire. There is also the lack of qualified and experienced personnel to code, hack, and battle online against the hybrid threats. Therefore, the MoD should start cyber career paths among the various defense organizations and employ more initiatives such as the recently established cyber reservist pool, to retain experienced cyber experts, and prevent losing them to much more attractive financial civilian contracts.

SOF have agile, adaptable, stealthy, flexible, and resilient personnel who could conduct independent and persistent operations. The SOF operators are culturally aware, speak the languages of countries they work in, and understand the environment in which they operate, including the risks and opportunities of that environment. They can be employed across the peace-war continuum in support of tactical, operational, and strategic level collection intelligence in both permissive and denied areas, with many available tools and capabilities. The drawbacks of SOF, though, are their insufficient cyber awareness and digital experience. They lack the technical background or simple coding skills. Due to their physical presence, they are also always at a higher risk than their cyber colleagues behind their desks back home.

To bridge the gap between the cyber experts and SOF operators, the mutual cultural understanding should be increased by cross-training, joint exercises, and untimely operations. Good command and control, excellent leadership, the proper legal framework, and clear communication is not enough. Both SOF and cyber personnel should also interact more often with each other and learn the basic techniques for SOF and cyber operations. Both should plan together, enjoy sports and recreation together, work together, and broaden their scope of life and get rid of the horizontal and vertical boundaries to prevent stovepipe thinking.

The three SOF-cyber integration options reveal that various options could start simultaneously from a decentralized SOF cyber personnel integration in both tactical-operational levels with KCT and NLMARSOF. Meanwhile the integration initiative already begun on the strategic level among SOCOM, DCC, and JSCU, with integral planning and the use of liaisons, can grow. It is important to keep in mind that all integration options demand an open and unbiased view, mutual respect, clear communication, and the will to start small with simple and inexpensive cyber capabilities. Until the political climate is ready for offensive cyber operations supported by SOF, the MoD leadership should seek opportunities in the current legal framework with intelligence, MKSO, or Article 100 procedures.

The strategic utility of special operations has the potential for innovation, and the role to support cyber operations is one of them. SOF must be considered in relation to, and as a tool of, an overall national or coalition strategy to support cyber operations. Even so, tactical excellence on the ground with KCT and NLMARSOF is no guarantee of strategic effectiveness. Therefore, integral planning and communication, mutual understanding, and cultural awareness is key for an effective and efficient use of SOF and cyber capabilities to make that combined fist against the hybrid threats the Netherlands is currently facing.

D. THE WAY AHEAD

In 2021, the new tri-national special forces command consisting of Belgium, Denmark, and the Netherlands will be fully operational and on stand-by as a NATO

Response Force (NRF) with NATO SOF capabilities.[175] This command, better known as the C-SOCC, was created in line with NATO's ambitions to fill the shortfalls in small European countries for conducting SOF operations. The NATO special operations headquarters (NSHQ) in Mons, Belgium, facilitates, supports, and advises to synchronize the C-SOCC activities with NATO regulations, doctrine, and procedures.[176]

Meanwhile, the multinational and interdisciplinary NATO Cooperative Cyber Defense Centre of Excellence (CCDCEO) in Tallinn, Estonia, acts as the cyber defense hub for NATO countries.[177] The CCDCEO organizes congresses and exercises on cyber conflicts and their relevant issues, and develops and writes cyber strategy like the *Tallinn Manual 2.0*.[178] Despite plans to increase the cooperation among NATO SOF partners and the CCDCEO, however, there is no direct cyber link to the NATO SOF allies, with the NSHQ in particular.[179]

Both SOF and cyber capabilities are scarce, precious, and effective national strategic assets, which NATO countries are not easily willing to share. Therefore, an integration effort between NATO SOF and cyber allies, to support NATO cyber operations, will be an ambitious and abiding process. In consequence, the C-SOCC has provided three small European countries with opportunities to experiment and practice with their SOF and cyber capabilities. This tri-national test case has provided operations for other NATO SOF and cyber countries to learn. So, the signatures of the Belgian, Danish, and Dutch defense

---

[175] NATO, "Three Allies Establish Special Forces Command, 07-Jun.-2018," accessed August 13, 2019, https://www.nato.int/cps/en/natohq/news_155347.htm.

[176] NATO.

[177] CCDCOE, "The NATO Cooperative Cyber Defense Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defense Expertise," accessed August 13, 2019, https://ccdcoe.org/.

[178] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (New York: Cambridge University Press, 2017).

[179] Email contact between senior staff officer Lieutenant-Colonel Theo Mestrini NSHQ and the author of this thesis, October 22, 2019.

ministers at the NATO headquarters in Brussels, on June 7, 2018,[180] could be the start to provide NATO with a composite command combining SOF and cyber capabilities. Shared lessons learned from each C-SOCC participating country about their SOF and cyber integration can be incorporated to smooth the process of SOF and cyber cooperation among Belgium, Denmark, and the Netherlands.

On the national level, political-strategic leaders inside the MoD are not doing enough to create an environment that is conducive to SOF and cyber capability integration. During the thesis interview, director Joint SIGINT Cyber Unit Marc Brinkman explained: "The political military-strategic level should set up a research and development environment where SOF and cyber could experiment, facilitate, test, develop, and innovate to create the right conditions to set the SOF cyber integration up for success."[181] In short, the senior MoD leadership should set the conditions that promote better and deeper integration between SOF and cyber capabilities by establishing a clear directive with national guidance. MoD leadership need not search for the solutions, but instead create the fertile conditions and simply listen to their SOF and cyber specialists to promote the SOF and cyber integration, synchronization, and cooperation.

As mentioned by President Richard Nixon, "If you want to make beautiful music, you must play the black and the white notes together."[182] The same is relevant for defeating the current hybrid cyber threats the Netherlands is facing; SOF and cyber capabilities should more integrated and should collaborate to enhance their effectiveness and efficiency. As the need for cyber operations continues to grow, SOF can support this online warfare expansion by filling the physical gaps to make these cyber operations more successful. Despite the different cultural backgrounds of SOF and cyber personnel and the various dynamics and conditions that influence the actual integration, it is crucial to play

---

180 "Rol Nederland bij Speciale Operaties NAVO" [Dutch Role in NATO Special Operations], *Telegraaf*, June 7, 2018, https://www.telegraaf.nl/nieuws/2142376/rol-nederland-bij-speciale-operaties-navo.

181 Interview with director Joint SIGINT Cyber Unit, The Hague, September 9, 2019.

182 Nixon, "The Quotable Richard Nixon."

the national SOF and cyber ‘notes’ together and play beautiful music to resist and hopefully counter the national and future NATO hybrid cyber threats.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. INTERVIEWS WITH SOF AND CYBER EXPERTS IN THE NETHERLANDS

Interview with Commander NLD Special Operations Command (SOCOM) MG Ten Haaf and cyber advisor Defense Operations and SOCOM LTC Wens
Monday 09 September, 2019 1300–1400

One reason for this interview is to provide a feasibility check on whether the three pillars used in the Naval Postgraduate School (NPS) thesis are suitable for Dutch SOF with the Defensive Cyber Command (DCC) via an article 100 operation, the *Ministeriële Kerngroep Speciale Operaties* (MKSO) procedure, and Joint SIGINT Cyber Unit (JSCU) through intelligence operations. In general, the ground roles for cyber to support SOF are in a defensive, offensive, or Intelligence Surveillance and Reconnaissance (ISR) posture. One needs to make a clear difference between SOF supporting cyber operations (DCC supported by SOCOM) and cyber supporting SOF operations (SOCOM supported by commander DCC). This flexibility of command relationship should be always possible. However, keep an eye on the fact that SOCOM and DCC are in a starting phase with fewer experiences in these joined combined cyber SOF operations.

The future battlespace will be in a multi-domain and hybrid environment. SOF and cyber are part of a hybrid environment and can be used as one tool in a toolbox with many options. When we are looking at SOF and cyber operations, we should consider the whole process from the starting point to the end of the operation when the evaluation is finished. Currently, we see that cyber is integrated too late into the planning process. Therefore, both DCC and SOCOM have liaisons in each other's organizations by changing their physical work location. A practical example is that the SOCOM cyber advisor is detached for a couple of days a week at the DCC and vice versa. SOCOM has had good experiences by using this construction with the Military Intelligence & Security Service (MISS). Using this structure makes it possible to keep each other well informed and react promptly when things look to go wrong and give a mutual understanding of both organizations' thoughts. When we conduct an operation, it is ultimately the Chief of Defense (CHoD) who gives

the order, after advice from his subordinate commanders, and gives the command and control guidance for SOCOM and DCC.

We have foreseeable and non-foreseeable operations within SOCOM, and we follow the normal lines of operations without leaving the common MoD procedures. Proven command relationships should not be changed. This keeps the decision making clear and consistent.

The most important point between SOF and cyber is a cultural change. For example, we had a SOCOM-led exercise where cyber capabilities and personnel were integrated. The SOF approach is kinetic thinking and very fast in how to solve the problem, while the cyber specialist thinks longer, waits, and finally sees opportunities. For example, the high-security awareness of the exercise enemy created opportunities for the cyber personnel. By sending some manipulated emails into the enemy inbox with false American telephone numbers and information, the problem could be resolved by deceiving the enemy, which led to internal enemy distrust and unrest. This cultural difference between SOF and cyber personnel must also be clear for cyber specialists. Especially in operations, the cyber specialist needs to gain awareness into the SOF cultural mindset and understand what the needs are for the SOF operators.

DCC is not only for supporting SOF. We are new as SOCOM [established in December 2018] and on the commander's level, we are already well tuned in. Both SOCOM and DCC think the same about our roles. On the lower level, we have the liaisons, and cyber personnel have followed the same SOF planning courses to better understand the process of planning of a SOF operation. Therefore, in our current planning for a new French-led mission in Mali, we as SOCOM plan in close conjunction with our cyber partners from the DCC. We just send an information letter to the Dutch government about what we can do with what capabilities within the SOF and cyber domain. The French invited 12 countries including the Netherlands to establish a Combined Joint Special Operation Task Force (CJSOTF) in Mali. Right now, we are in the planning phase, including the courses of action development with the DCC and examining what cyber capabilities can be integrated into SOF operations.

At SOCOM we look at our taskings, authorizations, and responsibilities with a flexible mindset able to flip from supported to supporting command. Within the three available options to conduct SOF operations (article 100 letter, MKSO procedure, and intelligence operations via the WIV), it is vital to see the second- and third-order side effects within a planned SOF operation and always guarantee proportionality.

The Composite Special Operations Component Command (C-SOCC) allows SOCOM to work closer together with other NATO partners and exchange their experiences and knowledge about the SOF cyber integration during NATO exercises and operations.

[After the interview, I received the following written feedback on the summary and thesis questions from the cyber advisor Defense Operations and SOCOM LTC Wens.]

This thesis has an interesting approach to improve national cyber capabilities using SOF to combat the current hybrid threat. This is an opposite approach to the Dutch development in which cyber (emphatically) develops and is used as an enabler for military operations including SOF operations.

The research question focuses on SOF as an enabler for cyber operations and/or the development of cyber capabilities in favor of (future) SOF operations. [LTC Wens] does not know if this is a typical U.S. approach. The thesis topic can certainly lead to insights to promote one's development. It also gives insight into the American development of SOF and cyber influences. We see the same development within NATO (*NATO AJP 3.22 Military Cyberspace Operations*).

[LTC Wens] missed the equivalent reciprocity between SOF and cyber as it is now being shaped between DCC, MISS, and SOCOM—both in the development of complementary capacities and the integrated deployment of both capacities. In short, in [LTC Wens'] opinion, the development of SOF is inextricably linked to operating in the digital domain and/or via the digital domain using new technologies (including defensive,

offensive, intellectual cyber capabilities, AI, machine learning, big data, deep-fake, data-science, IGO, etc.).

What is the hybrid threat and what form does it take? This should worth be investigating. Because SOF, whether in combination with cyber capabilities or not, does not by definition have to be the correct or only answer to prevent the use of "all instruments of power" (often under the threshold of violence of Article 5) of a potential opponent.

Given the current state of development of the DCC and the recently started cooperation with SOCOM, it is more realistic to view the offensive capacities of the DCC in collaboration with the MISS and the JSCU as an enabler for future SOF operations to make it even faster, more efficient, and effective. The combination of SOF and cyber capabilities broaden the range of instruments of the Dutch armed forces and offer more options for actions in the various phases of conflict, including the pre-conflict phase (phase 0).

Depending on the desired cyber effect in support of SOF operations, the relevant cyber organizations (DCC, JCSU, DCSC) must be involved as quickly as possible in the preparation and planning of a SOF operation to achieve the desired tooling for development and preparations.

Time is, therefore, an important precondition, even a critical success factor. To obtain specific information or intelligence, as the development of specific tooling, is time consuming.

Similarly, the legal aspects in favor of (1) the necessary preparation (including building up information position, defining the digital footprint, determining targeting list, determining cyber-defined defended asset list risk assessment own C4I, gathering specific information or intelligence, (2) the development of tooling, and (3) the integrated planning for the deployment of desired cyber effects in support of a SOF operation.

These legal aspects not only apply to the gathering of intelligence or the development of offensive cyber capabilities, but also to the development and preparation of the defensive cyber capabilities (i.e., Defense Cyber Security Center of the Joint Information Provision Commando) for the protection and security of the own SOF C4I. In

short, it is not only about power projection (the use of cyber capabilities to influence the opponent), but also attention to preventive (protective) measures to enable SOF operations in and via the digital domain; in favor of, among others, Force Protection, Freedom of Action, and ultimately, mission assurance / success, regardless of the type of SOF operation such as MA, SR, or DA.

Interview with Jelle Haaster, Cyber Defense expert
Monday 09 September 2019 1500–1600

Jelle explained briefly the various levels of cyber responsibilities and their capabilities. At the strategic level, there are the DCC, MISS, GISS, and JSCU; then the operational level, with the Navy, Air Force, and Army with their Cyber Warfare Teams, and the Military Police with their HIT/DO teams. Finally, there is the tactical level where now only the Army SOF is active with imagery catchers.

On the tactical level, the SOF cyber integration works with LNOs and cyber reservists working for both KCT and NL MARSOF. SOF is developing the communication for the 20th century.

In a non-permissive environment, the physical security of cyber teams on the ground could be facilitated by SOF. However, there could be an overlap with the HUMINT operators of the MISS, which should be deconflicted. But SOF could have a role to support cyber operations like those explained in this thesis. A simple example, which Jelle explains, is using humans [could be SOF or HUMINT operators] who employ imagery catchers or social engineers, and using observation teams to film persons typing their codes on a smartphone or other device, which could prevent long and expensive hacking sessions.

DCC has insufficient cyber capabilities and qualified and trained personnel to support the MoD on the tactical and operational levels. Therefore, they only conduct operations on a strategic level, which results in the Operational Commands (OPCOs) starting their cyber warfare teams separately from each other. Yet, 99 percent of the current cyber operations the Netherlands is conducting are intel exploitation operations under the wings of the JSCU and not the offensive cyber operations executed by the DCC. This is also a reason why many cyber personnel are leaving the DCC and working for the cyber desks of the MISS, GISS, or the JSCU itself. Although these organizations conduct no offensive cyber operations, the work and capabilities are a lot more dynamic and interesting. Since it started five years ago, however, with and an annual budget of 75 million euros, the DCC should start producing by delivering products and services to the

MoD organization. This is the main thesis in the NRC journal article of December 5, 2018. Bottom line, offensive cyber operations are difficult to conduct and organize.

The MoD needs better cyber awareness on all levels and in all military organizations. Therefore, the new whitepaper A-700 will give direction for all MoD personnel to be more cyber-aware by following lessons in operational, personnel, and force security.

The Netherlands has very sophisticated military cyber hackers and capabilities, which can be easily used for SOF on tactical levels. Simple, inexpensive equipment like the pineapple, which was used in the OPCW hack by the Russians, can be bought for less than 10,000 Euros and be used as interception means for low tactical SOF operations. Plus, the huge data centers and connection nodes in Amsterdam provide the MISS and GISS plenty of opportunities.

Interview Commander Joint SIGINT Cyber Unit Marc Brinkman
Monday 09 September 2019 1600–1700

After hearing that this thesis describes three options to support cyber operations, Marc Brinkman agreed that these options are suitable for SOF including the role as quick reaction force when a cyber technician needs to be extracted or when somebody pushes the "red-cyber-button." Next, Marc made the following recommendations and observations about the role of Dutch SOF to support cyber operations:

The technology of encryption and security of data and networks in the cyber domain gets better and tighter every day. Data density is increasing, with Amsterdam as a global data center and crossing point for data traffic growing and growing. Therefore, it is more difficult to find mazes in the net to search for opportunities and vulnerabilities to exploit by cyber and the Joint SIGINT Cyber Unit (JSCU) in particular. Everybody [military and intelligence cyber personnel] is searching for that same gap or bug in the system to exploit.

The current cyber orientation is more focused on interception on devices (smartphones, iPads, laptops, etc.) and less on general networks. To intercept signals and data on devices the actor needs to be closer to the device and its user. Especially, 4G, 5G, and the future 6G networks require a very close distance to the device.

The political-strategic level in the MoD is not doing enough to create an environment where SOF and cyber can integrate. Command and control (C2) should set the conditions that promote better and deeper integral integration between SOF and cyber. To benefit from the power of the integration of SOF and cyber, C2 needs to establish a clear direction, guidance, and conditions. The military C2 need not search for the solutions, but instead leave that to the SOF and cyber specialists, and not put it on the operational (OPCO) level. To promote the SOF and cyber integration, synchronization, and cooperation, the military C2 from SOCOM and DCC need to establish cyber SOF consultations periodically.

Use C-SOCC as an opportunity to share experience, knowledge, and techniques between Denmark, Belgium, and the Netherlands. It is a perfect test case for NATO SOF

and cyber to integrate combined tri-national procedures. Other NATO SOF and cyber countries could learn from the C-SOCC experiences. For the JSCU, Denmark is already a preferred partner, sharing intense cooperation and collaboration between cyber experts.

The political military-strategic level should set up a research and development environment where SOF and cyber could experiment, facilitate, test, develop, and innovate to create the right conditions to set the SOF cyber integration up for success.

Interview Commander NLD Defense Cyber Command Commodore
Boekholt O'Sullivan
Tuesday 10 September 2019 0900–1030

Commodore Boekholt O'Sullivan first gave an overview of the current status and activities of the Defense Cyber Command. Although the DCC has been in existence five years now, it is still in the process of developing and growing into a mature organization with well-equipped and educated personnel. The first four years the DCC has been focused purely on innovation, but now the accent has changed to professionalization. The DCC makes digital weapons to destroy enemy networks, devices, or digital infrastructure. DCC's main product is the delivering of cyber mission teams who work on the strategic level with both NLD SOCOM and the MISS. The center of gravity for the DCC is the shaping of operations with deception, deterrence, and influence. Nevertheless, the current Dutch political climate does not seem ready for the use of offensive cyber weapons in this form. Moreover, there is no legal framework yet, which means that the DCC have to conduct operations under the wings of another authority. Therefore, the DCC is currently acting more as an employment agency for the MISS and JSCU. This is not an issue for the commander DCC. If there is a good reason and it benefits the MoD, she is even willing to use future reinforcement by personnel expansion and detach it to the operational commands.

Because the DCC lacks its legal mandate, and the political climate in the Netherlands is not ready yet to conduct offensive cyber operations under the wings of an article 100 letter, DCC can only loan personnel via the *Wet Inlichtingen Veiligheid* (WIV) to the MISS and JSCU. Yet, the MKSO procedure will soon be adjusted to involve offensive cyber operations executed by the DCC.

To integrate DCC and SOCOM there are liaison officers from SOCOM working in the DCC and vice versa. This generates empathy and imagination in both organizations. The SOCOM liaison is placed in the future OPS J5 cell of the DCC to make sure that the liaison can always think of how to implement SOF and cyber capabilities in future scenarios and ultimately real-time missions. This is different within the J3 current OPS

cell, where everything is executed as it arrived, without the possibility of influencing the process, effects, and the end state.

SOCOM is short-term focused, while DCC is more oriented on a longer period. SOF personnel need to slow down in their decision-making versus DCC, which could learn to accelerate in its process or at least explain to SOF to slow down. An example is that SOF wants to shut down a security camera on a particular object to conduct a direct action, while cyber experts think more about the second- and third-order side effects. Together they should develop scenarios that use both SOF and cyber capabilities. The biggest gap between SOCOM and DCC is the lack of imagination between these two organizations. Both worlds have extremely different personnel and cultures, and need time and effort to integrate. Each should show real interest in the other to bridge the gap between the "cyber nerd" and kinetic-oriented SOF operator.

The human factor such as agents or SOF is necessary for placing digital means in a permissive or semi-permissive environment. Therefore, this NPS study could potentially provide the DCC and SOCOM options and solutions on how to integrate SOF and cyber for use in scenarios and ultimately during real-time missions.

The young and highly motivated cyber experts within the DCC are having problems with the current mandate and its legal framework. Lawyers are blocking the cyber experts' imagination, improvisation, and creativity which are necessary for future cyber scenarios.

The strategic cooperation among DCC, SOCOM, and the intelligence services (MISS and GISS) is in a starting period. The tendency to overclassify documents, scenarios, and exercises makes it difficult to break down the walls between the compartmentation, which is necessary for fruitful cooperation. Not everything has to be labeled as secret. Therefore, DCC, SOCOM, and the intelligence services need to educate each other. But again, DCC is now primarily in a supporting role due to the current political climate in the Netherlands. When DCC is more mature this could change in a supported role.

Intelligence services share information with other friendly services to gain new information. This exchange is a method for intelligence collection. The DCC cannot

exchange zero exploits or other means with foreign-friendly cyber organizations. Therefore, everything has to be developed within the DCC's own management. The DCC can help with the growth of the intelligence services, however, by placing cyber mission teams into the JSCU or the MISS itself.

Cyber offensive operations are very difficult to execute in the current political climate. The defensive cyber operations are focused on their own computer system security and threat hunting, as well as knowing what the threat is, who the actor is, and what the possibilities are to terminate the digital threat.

Commodore Boekholt O'Sullivan stressed the importance of a serious integration between SOF and cyber capabilities. The DCC can only develop into a mature cyber organization by cooperation with others. The DCC cannot do everything; they are no cyber commandos (despite being called that by the Minister of Defense), and the DCC personnel should be loyal to their values and believe in what they are doing. By not integrating the physical and virtual domains, the DCC puts itself in a situation where it cannot develop.

The three options for integration mentioned in this NPS thesis should be further investigated. The three roles for Dutch SOF to support cyber operations make sense for the DCC and give opportunities for the DCC's current development. Furthermore, the command and control should be executed via a supporting or supported relationship. Due to it being a young organization, the DCC is still in a development phase and less experienced with real-time missions. Therefore, the Dutch SOCOM should take the lead. This supporting role allows the DCC to learn and focus on the next level and create an operations-focused staff including a new chief of staff. The lessons identified and learned should be implemented in the DCC, which can give cyber personnel possibilities to think about and accelerate their work.

The current Chief of Defense Admiral Bauer took the DCC from under the operational umbrella of the Army and put it next to SOCOM and the four operational commands on the strategic level. This MoD measure made it possible for the DCC to think about the future and implement cyber capabilities from the beginning.

Although the DCC and JSCU are only acting on the strategic level, there are now movements on the operational-tactical level to establish cyber warfare teams. Every operational command requests 30 to 40 cyber experts. In turn, the DCC is asking simple questions: What are they doing and for what reasons? Right now, there is no clear and consistent plan or mission, and therefore, stovepipe thinking among the various operational commands is a risk. Consequently, the four operational commands need to sit down together with the DCC and build a transparent vision with various levels with fewer boundaries and restrictions, instead of setting up own cyber demands on the private market. In the end, it is all about what effects the operational commands want to achieve with the cyber warfare teams.

Interview with operational manager crypto Fox-IT Daniël Datau
Tuesday 10 September 2019 1230–1330

It makes sense for ex-military Daniël Datau to further investigate the three NPS thesis pillars for SOF to support cyber operations. Such an assessment depends on the context and goals. The DCC is in the lead to achieve these goals on a strategic level. Therefore, Daniel has proposed for the operational-tactical level to establish a local decentralized cyber capability that allows the Dutch SOF community to conduct SOF-cyber missions, which are initiated from the bottom-up.

With the proper mandate and legal framework, cyber capabilities can achieve serious results. It is not a question of whether these cyber capabilities can achieve results, but when they can start with the proper infrastructure in place. In military intelligence cyber operations, many things and techniques are possible. These same standard techniques and capabilities could be used for offensive cyber operations when the correct mandate is established. The MoD has top of the bill hackers who are very capable in offensive cyber operations. The conditions, however, are not ready yet. Plus, the DCC is in its current organization too ambitious to do everything.

The MoD and the DCC, in particular, have issues keeping the well-experienced hackers on board. They could make much more money in civil organizations like, for example, Fox-It. The pool of cyber reservists the DCC is currently using is a good start for the strategic level, but on the operational-tactical level, Dutch SOF should just start with own cyber capabilities and personnel.

Countries such as China and Russia are more advanced in offensive cyber operations on the operational-tactical level than the pacifistic Netherlands, which is not willing to take the risk with offensive cyber operations. On the other hand, the Dutch MoD is very good at signaling, but the next step in the cyber process is less developed. Many official reports and white papers are written about these cyber issues, but nobody has given the thumbs up to start with decentralizing organized cyber operations within the Dutch SOF (KCT and NLMARSOF).

This decentralized organization of cyber capabilities and personnel could benefit both KCT and NLMARSOF. By investing only a few hundred thousand euros, the Netherlands could obtain imagery catchers, pineapple machines, and other simple digital interception devices for use in joint SOF cyber operations. In addition to procuring such devices, knowledgeable personnel will be needed to operate those devices. For security reasons, it is important that a hacker should not become a SOF operator or vice versa. Therefore, it is sometimes easier to rent commercial personnel or put temporary cyber enablers in SOF teams.

To organize operational-tactical level cyber capabilities, the operational commands with their SOF units could use enablers or reach out to facilities back in the Netherlands. However, this organization should start small, and personnel need to train, exercise, and work together to educate and learn from each other. Do not make it too difficult and use proven facilities, capabilities, and infrastructure from commercial cyber companies.

Although there are many possible options to integrate SOF and cyber capabilities, the third option from the NPS thesis is suitable depending on the goals and missions. This option with cyber-enabled special warfare teams should be based on mutual understanding and sufficient cyber awareness. These cyber-enabled special warfare teams should train in the detection and signaling of digital vulnerabilities in networks. The teams could also use COTS and inexpensive tools for interception and detection. By exploiting these cyber signals, it is possible to collect intelligence. Operators on the ground could use an application to intercept MAC addresses, IP accounts, Wi-Fi-networks, and see where mobile devices log in and register on local signal towers.

Hackers are always dependent on physical surveillance and interaction. SOF's boots on the ground could provide these opportunities. Therefore, this NPS thesis could be valuable for further investigation.

There is a large difference between the planning and execution of SOF and cyber operations. It does not matter what planning process model is used, such as the cyber kill chain or the Fox-IT red teaming; there is always a spiral planning cycle. SOF plans phase after phase. First, conditions need to be in place before the next phase can be activated and

ultimately the actual action can happen. By contrast, in cyber operations something has already happened in the first phase, without creating the conditions. Despite this difference, the character of SOF and cyber operations is almost identical. Both can operate stealthily, under the radar, and in a clandestine way, without generating lots of collateral damage.

For Fox-IT, all three integration options proposed in this NPS thesis are suitable for support. Fox-It can deliver low cost, inexpensive capabilities, and the necessary education. It could also provide a kick start for the MoD and show what will work but also what will not work, without requiring large budgets or long training projects.

Interview director crypto Fox-IT Jurgen Delfos
Tuesday 10 September 2019 1400–1500

Fox-IT is responsible for the encryption of classified data of corporate businesses, smaller companies, and non-governmental and governmental organizations in the Netherlands and abroad. Having strict ethical standards, Fox-IT does not want to provide services to foreign organizations and regimes where human rights are being violated. Sometimes Fox struggles with the decision to support a country or organization because of competition from Israel and the United States for data encryption, such as with Datadiodes. Yet, saying no can also give a competitive advantage to an honest, transparent, and reliable company. Fox-IT is not allowed to conduct offensive cyber operations, although the line between offensive and defensive gets a bit blurry at times.

For the MoD, Fox-IT provides cyber technology and supports large communication projects to secure the lines of communication among the various stakeholders. Since the Edward Snowden scandal, security no longer focuses only on threats coming from the East, but from everywhere. By developing countermeasures, white hackers from Fox secure and support high-value targets and large key management information systems within the MoD.

Luckily, the MoD understands the urgency to establish good security and countermeasures to prevent hacks that could turn MoD systems into weapons. Fox-IT and MoD together conduct a strategic crypto development without exactly knowing what the output and end state will be. Nonetheless, the MoD has allocated a budget with DMO and JIVC, and shown courage and vigor in making this development happen. Within the acquisition and finance department of the MoD, legality always takes precedence over efficiency. This was the case when the MoD requested a new purchasing policy. In other words, it was deemed better to spend one million euros for nothing if it was legal, than to spend 100,000 euros wisely but not in accordance with the European regulations.

The MoD is accountable for the tax money it spends and therefore needs to follow the rules and regulations applicable for buying equipment and systems. At the same time, however, the uncertainties in the cybersecurity environment are growing, processes are

going faster, and purchasing is lagging behind. If zero-days exploits are not up-to-date, the MoD systems are in danger. This requires complex contracts and structures between Fox-IT and the MoD.

With the right equipment, a physical component like SOF could have valuable effects for security in the cyber domain by gaining access to important digital infrastructure.

Interview Commander NLMARSOF LTCOL Jan-Willem van Dijk
Thursday 26 September 2019 1100–1130

Of course, commander NLMARSOF would like to have his cyber capabilities in house. Yet, these cyber capabilities are specialized and intimidating. And, it is unrealistic to find all these skills [SOF and cyber] and expertise in one single person. Therefore, NLMARSOF needs cyber specialists, but the question is how can it meet these staffing needs?

Cyber personnel encompass many specialists and experts; consequently, it is not possible to train, educate, and teach own NLMARSOF operators or staff in this domain as well. That is why NLMARSOF will be depending on external organizations. However, it is not always possible to receive these supporting cyber capabilities, because it is a scarce asset. Therefore, one should organize an interface between the user and the supplier. NLMARSOF needs own personnel with a better understanding of cyber operations, to link and liaise with the cyber organizations that have rare cyber capabilities. This link is already operational with the JSCU and makes it possible to bring these cyber capabilities into the theatre during real-time operations.

NLMARSOF only needs to bring in their capabilities to transport cyber personnel via the air, land, and water into an operation area. Especially the maritime domain gives opportunities for SOF to covertly insert or extract cyber personnel from the intelligence services such as the MISS and the GISS. Within this maritime domain, the underwater option is almost the last resort to bring a person to a covert location. In these infiltration and exfiltration opportunities, NLMARSOF is the facilitator or enabler, but cannot create these cyber effects independently.

Cyber is an effect generated from a physical distance. When this is not possible from a distance, however, SOF's role can be to plug in a USB stick or bring in a hacker to conduct the cyber operation closer to the object. The effect NLMARSOF can gain from cyber operations is to create more cyber awareness and be able to conduct simple cyber interception operations that include the use of the necessary tools.

Currently, cyber awareness within NLMARSOF is trained in LVO—being invisible not only in the physical environment with the right camouflage but also in the information domain by trying to avoid a signature. Detecting an actor's attempt to remain invisible in the information domain requires paying attention to someone's electronic warfare signature, use of burner phones, or use of a blue and red network. These techniques are also needed in conventional warfare. Lessons learned in the cyber domain are applicable for operations in the conventional domain.

NLMARSOF uses its interface with JSCU and the intelligence services to learn more about how to be digitally invisible to support conventional warfare and intelligence services. By using simple interception devices and imagery catchers NLMARSOF is already able to support cyber operations. The LVO teams are using the interface with cyber to learn in their operations how to support conventional operations and the intelligence services.

The intelligence services that are acting on a strategic level are dealing with tactical information. That same tactical information is useful for the tactical units on the ground like NLMARSOF. To receive this tactical information, one should be part of the intelligence network. Yet, this is not the official way of receiving information. Furthermore, it is complicated to formalize this procedure, due to stovepipe thinking and bureaucracy in the MoD. The available information is useful and interesting for all three levels [tactical, operational, strategic]; however, it is only available for the strategic level. Even on a political level, it is not acceptable that when the information is available on the strategic level in a particular country, SOF operators are excluded from this information when operating at the tactical level in the same environment and dealing with the same risks. Therefore, communication lines should be put in place to make sure the available information reaches all levels that are involved. The role of SOCOM is precisely to interface and liaise with the intelligence services, JSCU, and the SOF units. The connection between SOCOM and the MISS is therefore crucial.

The operational commands are still an extra layer between the strategic services like SOCOM, DCC, and intelligence services, including JSCU and the SOF units. To close the information loop between the strategic and tactical level [such as KCT and

NLMARSOF], the operational commands need more capacity. In NLMARSOF's case, the Navy is currently another stovepipe that prevents a clear information communication line. The Navy intelligence organization is growing but is still not able to bridge the information gap between the strategic intelligence services and tactical NLMARSOF. Nevertheless, the Navy is busy connecting the various levels with extra personnel and money to close the information loop.

NLMARSOF and KCT are both SOF units working under the umbrella of SOCOM. There should be no difference between these SOF units. They should be able to work jointly together in various settings and conditions without any barriers. It is possible to have own courses and training pipelines within both KCT and NLMARSOF. This is not an option for cyber capabilities, however, because the Netherlands is too small for separate cyber tracks.

To realize a better integration between SOF and cyber, the Navy with NLMARSOF, in particular, uses liaison officers at SOCOM, JSCU, and the MISS. This liaison network is the external interface NLMARSOF is using besides the internal interface with own LVO operators and project officers. Both interfaces [internal and external] connect all the various pillars within the MoD. To stimulate this integration, mutual exercises with SOF and cyber are needed. These exercises show that the stovepipes among the various stakeholders in the SOF, cyber, and intelligence domain should be pulled down.

Written Response Interview Questions Commander KCT COL Rene van den Berg
Tuesday 26 November 2019

1. *What are the current cooperation, coordination, and separation of SOF and cyber capabilities?*

At the tactical level, within exercises, there is cooperation with DCC. Coordination is directed from the KCT to the Cyber Command. This runs through a DCC liaison officer. Separation of SOF and cyber capabilities between KCT and DCC are mainly on the skills and knowledge level.

2. *What are the future cooperation, coordination, and separation of SOF and cyber capabilities?*

Cyber capacity should be integrated within the KCT to support SOF operations. Ultimately, cross-functional SOF teams should be created among other cyber capacities such as operators, are integrated. Then there is no longer the question of cooperation but more of a symbiosis. SOF is responsible for the coordination, with separation at the tactical team level and different capabilities existing within every SOF operation.

3. *What are the gaps between SOF operations and cyber capabilities and vice versa?*

Current SOF operations are primarily focused on the physical and cognitive dimensions. The influence of SOF actions and the human behavior of SOF operators plus its effects within the virtual dimension is not fully clear yet. Moreover, consciously performing SOF operations within the virtual dimension, or using the virtual dimension to create effects, is in SOF operations currently uncertain. Cyber capabilities are also not specifically designed to support or execute solely SOF operations.

4. *What is the strength of SOF and cyber capabilities combined?*

The strength is to accelerate and increase situational awareness and understanding. Combining SOF and cyber capabilities reduces the physical footprint in preparation for a possible direct action. It also generates extra special reconnaissance capabilities. In general, cyber capabilities within a hybrid situation allows to better understand and influence the situation. Therefore, well-integrated cyber capabilities within SOF will be a force multiplier.

5. *How can SOF support all three cyber operations (defensive, offensive, and intelligence exploration)?*

In a permissive and non-permissive environment, SOF can support cyber operations in various phases of a conflict, by physically placing digital assets such as software (virus or malware programs) or hardware (cameras, trackers, computers, etc.). Moreover, when necessary SOF can establish the connection locally from the placed devices back to the cyber experts. Besides, SOF can look for the physical confirmation of what cyber experts with their capabilities think is actionable intelligence within the virtual dimension.

6. *How can cyber support SOF in Military Assistance (MA), Direct Action (DA), and Special Reconnaissance (SR)?*

Within MA, cyber capabilities could map the digital network of a partner unit and investigate a possible insider threat. Within DA, hacking of digital systems in or around the target could result in actionable intelligence. This digital intelligence preparation of the environment supports the SR phase before the actual DA. During the direct action itself, cyber capabilities provide digital (near) real-time information of the object and the environment. Within SR, cyber capabilities digitally reconnaissance the SR target by collecting intelligence and information, and monitoring related social media developments. This could include hacking hardware to gain insight into the situation of the SR target.

7. *How can SOF and cyber capabilities be integrated?*

SOF and cyber can be integrated by integrating cyber capacity within SOF at all levels (strategic, operational, and tactical). In the KCT, this means a cyber section at the staff level in operations or intelligence, and cyber operators who can operate within the SOF teams at the tactical company level. This means that SOF operators must develop digital knowledge and skills to a certain level and cyber operators must develop certain SOF knowledge and skills. As a result, both capacities grow towards each other and could generate great effects.

8. *How could the physical and virtual domains reinforce each other?*

The physical and virtual domains could reinforce each other by taking an integrated approach. Currently, all physical actions affect the virtual dimension. A person leaves an indelible digital footprint. Also, actions (conscious and unconscious) in the virtual dimension influence the physical dimension and the actions or operations that somebody wants to perform physically. Separately approaching both dimensions is no longer an option. Cyber is a force multiplier for SOF operations and SOF can be the same for cyber operations if physical and cognitive actions are required.

9. *What does an integrated SOF-cyber operational concept look like?*

At the tactical level, cross-functional SOF teams with dedicated cyber operators should be available, including a tactical staff with a cyber section integrated within operations or intelligence (cyber is not just intelligence). On the operational level, there are cyber sections, and strategically there is already the DCC and the JCSU.

10. *What does an integrated SOF-cyber operational concept mean for the SOF organization and the role of NLD SOCOM?*

An integrated SOF-cyber operational concept means that SOF can perform full spectrum SOF operations within all dimensions: physical, cognitive, and virtual. Now, this is mainly happening within the physical and increasingly the cognitive dimensions. The virtual dimension is lagging. The role of NLD SOCOM is to realize this concept bottom-up. Currently, the biggest gain to achieve is at the tactical level and this will have an efficient spin-off towards the operational and strategic levels.

11. *What command and control relationship between SOF and cyber operations is used?*

At the moment, there is no command and control relationship between SOF and cyber. Within exercises where we experiment with cyber capabilities, the relationship is mainly tactical command (TACOM) and/or tactical control (TACON). In the ideal world, the full command should be embedded at all levels within the SOF cyber capacity.

12. *Did SOF and cyber cooperate in recent operations?* (Commander KCT has no insights on this).

- ***a.*** *If yes, on what level (strategic, operational, tactical)?*
- ***b.*** *What were the results?*
  - ***i.*** *Lessons learned (only unclassified)*
  - ***ii.*** *Lessons identified (only unclassified)*
- **c.** *What is doctrinal and technical published about SOF and cyber cooperation? (only unclassified)* Commander KCT does not know official publications except DTOS.
- ***d.*** *What are the opportunities for this cooperation?*

By being able to cover all three dimensions within SOF operations, SOF can achieve strategic effects more efficiently. Furthermore, it increases force protection,

situational awareness, and the understanding of how to apply the principles of hybrid warfare in a hybrid conflict or in a conflict with a near-peer competitor that can operate at a high level within the virtual dimension.

13. Which measures are taken by the MoD to prepare SOF and cyber capabilities for the hybrid threats/warfare?

No direct actions are known to me regarding the development of SOF and cyber. A Counter Hybrid Unit has been established at the defense staff level. This unit investigates what actions are needed to counter hybrid threats. I have no further insight into what has already been developed for this. However, it is not specifically aimed at SOF and cyber.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Antonovish, Pavel. *International Conflicts in Cyberspace: Battlefield of the 21st Century*. Washington, DC: U.S. Department of Defense, 2017.

Arquilla, John. "Perils of the Gray Zone: Paradigms Lost, Paradoxes Regained." *PRISM* 7, no. 3 (May 2018): 119–28.

Arquilla, John, and David Ronfeldt. "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 141–65. https://doi.org/10.1080/01495939308402915.

BBC News. "How the Dutch Foiled Russian 'Cyber-Attack' on OPCW," October 4, 2018. https://www.bbc.com/news/world-europe-45747472.

Bekkers, Frank, Rick Meesen, and Deborah Lassche. *Hybrid Conflicts: The New Normal?* The Hague: The Hague Centre for Strategic Studies and TNO, 2019. https://hcss.nl/report/hybrid-conflicts-new-normal.

Bijleveld-Schouten, A.Th.B. Officiële publicatie, Staten-Generaal der Tweede Kamer "Vaststelling van de begrotingsstaten van het Ministerie van Defensie (X) voor het jaar 2018 ; Brief regering; Reactie op verzoek commissie om inzicht in besluitvormings- en verantwoordingsproces inzake speciale en geheime operaties" [Determination of the Ministry of Defense Budget Statements for the year 2018; Government letter; Response to Committee's Request for Insight into Decision-Making and Accountability Process regarding Special and Secret Operations]. Officiële publicatie, Staten-Generaal Tweede Kamer der, March 27, 2018. https://zoek.officielebekendmakingen.nl/kst-34775-X-88.html.

Boersema, Wendelmoet. "Wat we Weten over de Russische Hackaanval tegen de OPCW" [What We Know about the Russian Hack against the OPCW]. Trouw, October 4, 2018. https://www.trouw.nl/home/wat-we-weten-over-de-russische-hackaanval-tegen-de-opcw~ad2eb078/.

Bouma, Floor. "Noodnummer 112 Urenlang niet Bereikbaar door KPN-storing" [Emergency number 911 Unavailable for Hours due to KPN Malfunction]. NRC. Accessed July 31, 2019. https://www.nrc.nl/nieuws/2019/06/24/noodnummers-niet-bereikbaar-door-landelijke-storing-kpn-a3964838.

Brown, Benjamin. "Expanding the Menu: The Case for CYBERSOC." *Small Wars Journal*, June 7, 2018. https://smallwarsjournal.com/jrnl/art/expanding-menu-case-cybersoc.

Buchanan, Ben. *The Cybersecurity Dilemma: Hacking, Trust and Fear between Nations*. New York, NY: Oxford University Press, 2017. https://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190665012.001.0001/acprof-9780190665012.

Bustra, Hans. *Security Leaks for Sale*. Zero Days VPRO Tegenlicht. VPRO, 2014. https://www.youtube.com/watch?v=JhkXSg9KQE8.

CCDCOE. "The NATO Cooperative Cyber Defence Centre of Excellence Is a Multinational and Interdisciplinary Hub of Cyber Defence Expertise." Accessed August 13, 2019. https://ccdcoe.org/.

CNN. "2016 Presidential Campaign Hacking Fast Facts," October 18, 2019. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html.

Corrin, Amber, Shawn McKay, Bob Murphy, Megan McKernan, Robert Warren Button, and Elliot Axelband. "Navy: Faster Acquisition Key to Cyber Defense." *FCW - Federal Computer Week*, June 28, 2011. https://fcw.com/articles/2011/06/28/cyber-warfare-summit-acquisition-reform-strategies.aspx.

Daft, Richard L., Jonathan Murphy, and Hugh Willmott. *Organization Theory and Design*. Mason, OH: Cengage Learning EMEA, 2014.

Department for Public Law, Jurisprudence and Legal History. *Veiligheid in een Wereld van Verbindingen: Een Strategische Visie op het Defensiebeleid* [Security in a World of Connections: A Strategic Vision of Defense Policy]. WRR-Rapport nr. 98. The Hague: WRR, 2017. https://research.tilburguniversity.edu/en/publications/82b3474a-edac-4a9e-97d6-af3a0807e17d.

Department of Homeland Security. *National Security Strategy of the United States of America 2017*. Washington, DC: Department of Homeland Security, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

Ducheine, Paul, and Ing. Kraesten Arnold. "Besluitvorming Bij Cyberoperaties." [Decision Making within Cyber Operations] *Militaire Spectator*, 2015. https://spectator.clingendael.org/pub/2016/6/_/pdf/IS_2016_6_duyvesteyn.pdf.

Duggan, Patrick M., and Elizabeth Oren. "U.S. Special Operations Forces in Cyberspace." *The Cyber Defense Review* 1, no. 2 (2016): 73–80.

Duggan, Patrick Michael. “SOF’s Cyber FRINGE.” *Small Wars Journal*, 2019: 1–9. https://smallwarsjournal.com/jrnl/art/sof%E2%80%99s-cyber-fringe

———. “Strategic Development of Special Warfare in Cyberspace.” *Joint Force Quarterly* 4th Quarter, no. 79 (October 2015). https://ndupress.ndu.edu/Media/News/Article/621123/strategic-development-of-special-warfare-in-cyberspace/.

———. “Why Special Operations Forces in U.S. Cyber-Warfare?” *The Cyber Defense Review*, January 8, 2016. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1136057/why-special-operations-forces-in-us-cyber-warfare/.

———.”The Unconventional Use of Cyber Between War and Peace.” Georgetown. Video, 0:06 Accessed May 24, 2019. https://www.youtube.com/watch?v=IFEE_nr8kYM.

Dutch Ministry of Defense. *Nederlandse Defensie Doctrine 2019* [Dutch Defense Doctrine 2019]. The Hague: Defensiestaf, 2019. https://www.defensie.nl/downloads/publicaties/2019/06/19/herziene-nederlandse-defensie-doctrine-ndd-2019.

———. “The Netherlands Armed Forces Doctrine for Military Cyberspace Operations.” Dutch Defense Cyber Command, February 2019.

Dutta, Soumitra, Bruno Lanvin, and Sacha Wunsch-Vincent. *Global Innovation Index 2018: Energizing the World with Innovation.* 11th ed. Cornell University, INSEAD, and the World Intellectual Property Organization. Geneva, Switzerland: World Intellectual Property Oranization, 2018. https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2018.pdf.

Eaton, Joshua. “Report: Dutch Security Services Infiltrated Russian DNC Hackers.” *ThinkProgress* (blog), January 27, 2018. https://thinkprogress.org/dutch-cozy-bear-hack-957b8d72bfd0/.

European Union. *Artificial Intelligence in Society*. Paris: OECD Publishing, 2019. https://ec.europa.eu/jrc/communities/sites/jrccties/files/eedfee77-en.pdf.

Factbook Korps Commandotroepen: Verleden - Heden - Toekomst [Factbook Army SOF: Past - Current - Future]. Roosendaal, Netherlands: Koninklijke Landmacht, 2014. https://www.korpscommandotroepen.nl/wp-content/uploads/2015/01/Factbook-KCT-2014.pdf.

Franceschi-Bicchierai, Lorenzo. “The History of Stuxnet: The World’s First True Cyberweapon - VICE.” Vice News. August 9, 2016. https://www.vice.com/en_us/article/ezp58m/the-history-of-stuxnet-the-worlds-first-true-cyberweapon-5886b74d80d84e45e7bd22ee.

Galeotti, Mark. “Hybrid War or Gibridnaya Voina? Getting Russia’s Non-Linear Military Challenge Right.” *Analysis and Assesments of Russian Crime and Security (blog)*, 2016. https://inmoscowsshadows.wordpress.com/2016/11/28/new-report-hybrid-war-or- gibridnaya-voina-getting-russias-non-linear-military-challenge-right/.

Gates, Robert M. “Helping Others Defend Themselves.” *Foreign Affairs*, June 2010. https://www.foreignaffairs.com/articles/2010-05-01/helping-others-defend-themselves.

Gibney, Alex. *Zero Days - YouTube*. Documentary, 1:57. Magnolia Pictures, 2016. https://www.youtube.com/watch?v=nnKdZyS3CKU.

Giegerich, Bastian, Bruno Tertrais, Sten Rynning, Casprini Federico, James Sperling, and Dick Bedford. *Managing Change: NATO’s Partnerships and Deterrence in a Globalised World*. Edited by Riccardo Alcaro and Sonia Lucarelli. Villa GuastaVillani, Bolonna, Italy: NATO Supreme Allied Command Transformation, 2011. http://www.act.nato.int/images/stories/events/2011/managing_change_hr.pdf.

Gray, Colin S. “Explorations in Strategy.” Westport, CT: Greenwood Press, 1996, Online Research Library: Questia. Accessed July 23, 2019. https://www.questia.com/library/1890059/explorations-in-strategy.

Graylog Blog. “Cyber Security: Understanding the 5 Phases of Intrusion.” Accessed July 18, 2019. https://www.graylog.org/post/cyber-security-understanding-the-5-phases-of-intrusion.

Guardian, “Dutch Will Count All Election Ballots by Hand to Thwart Hacking.” February 2, 2017. https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking.

Haaster, Jelle. “De Toekomst van de Landmacht met Jelle Haaster” [The Future of the Dutch Army with Jelle Haaster]. HCSS Podcast, MP3 audio, 0:12, Accessed March 3, 2019. https://podcasts.apple.com/us/podcast/hcss-podcast-toekomst-van-landmacht-met-jelle-van-haaster/id1274061866?i=1000427791939.

Haspels, Bernardus, and Flemming Elkjaer Haar. “The Strategic Utility of Small-State Special Operations Forces (SOF) as Information Collectors to Support National Decision-Making.” Capstone, Naval Postgraduate School, 2018. http://hdl.handle.net/10945/61378.

International Security Advisory Board. *Report on Gray Zone Conflict*. Washington, DC: U.S. Department of State, 2017. https://2009-2017.state.gov/t/avc/isab/266650.htm.

Jackson School of International Studies. “Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks.” Accessed July 22, 2019. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

Jasper, Scott. *Strategic Cyber Deterrence: The Active Cyber Defense Option*. London, UK: Rowman & Littlefield, 2017.

Jonker, Jorn, and Niels Rigter. “Meer Geld voor Defensie” [More Money for Defense]. *Telegraaf*, April 26, 2019. https://www.telegraaf.nl/nieuws/3503091/meer-geld-voor-defensie.

Kaufman, Joyce P. “The U.S. Perspective on NATO under Trump: Lessons of the Past and Prospects for the Future.” *International Affairs* 93, no. 2 (March 2017): 251–66. https://doi.org/10.1093/ia/iix009.

Kilcullen, David. *Out of the Mountains: The Coming Age of the Urban Guerrilla*. 4th ed. Vol. 25. Oxford; New York: Oxford University Press, 2013.

Kleining, Gerhard, and Harald Witt. “The Qualitative Heuristic Approach: A Methodology for Discovery in Psychology and the Social Sciences. Rediscovering the Method of Introspection as an Example.” *Forum: Qualitative Social Research* 1, no. 1 (January 2000). https://doi.org/10.17169/fqs-1.1.1123.

Koch, Robert, and Gabi Rodosek. *ECCWS2016-Proceedings of the 15th European Conference on Cyber Warfare and Security*. Academic Conferences and Publishing Limited, 2016.http://toc.proceedings.com/30838webtoc.pdf

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009. https://www.rand.org/pubs/monographs/MG877.html.

Loon, Marissa van. “Nog Eens Honderden Bedrijven Onbeveiligd Door Lek in VPN-Netwerk” [Once Again Hundreds of Companies Unsecure due to a Leak in the VPN Network]. NRC. September 29, 2019. https://www.nrc.nl/nieuws/2019/09/29/nog-eens-honderden-bedrijven-onbeveiligd-door-lek-in-vpn-netwerk-a3974981.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge, UK: Cambridge University Press, 2018. https://carnegieendowment.org/2018/01/18/cyber-mercenaries-state-hackers-and-power-pub-75280.

McRaven, William H. *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice*. New York: Presidio Press, 2009.

Miladinova, Vesela, Maarten Gehem, Peter Wijninga, Stephan de Spiegeleire, Frank Bekkers, Jasper Ginn, Jacques Mukena, and Nicolas Castellon. *Special Operations Forces: Schaduwkrijgers in Het Licht van de Toekomst* [Special Operations Forces: Shadow Warriors in The Light of the Future]. The Hague: The Hague Centre for Strategic Studies, 2015. https://hcss.nl/report/special-operations-forces-schaduwkrijgers-het-licht-van-de-toekomst.

Ministerie van Buitenlandse Zaken. *Wereldwijd voor een Veilig Nederland: Geïntegreerde Buitenland- en Veiligheidsstrategie 2018–2022*. [Worldwide a Secure Netherlands: Integrated Foreign and Security Strategy 2018–2022]. The Hague: Ministerie van Buitenlandse Zaken, 2018. https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs.

Ministerie van Justitie en Veiligheid. *Kamerbrief over maatregelen tegen statelijke dreigingen* [Letter to Parliament about Measures against State Threats]. Kamerstuk - Rijksoverheid, 2019. https://www.rijksoverheid.nl/documenten/kamerstukken/2019/04/18/tk-tegengaan-statelijke-dreigingen.

Ministry of Defense. *Defensie Cyber Strategie 2018: Inversteren in Digitale Slagkracht Voor Nederland* [Defense Cyber Strategy 2018: Investing in Digital Power for the Netherlands]. The Hague: Ministry of Defense, 2018. https://www.thehaguesecuritydelta.com/media/com_hsd/report/214/document/web-Brochure-Defensie-Cyber-Strategie.pdf.

Modderkolk, Huib. *Het is Oorlog maar Niemand die het Ziet* Huib Modderkolk, *Het is Oorlog maar Niemand die het Ziet* [It is War but Nobody Sees it]. 3rd ed. Amsterdam: Publisher Podium, 2019. http://www.letterenfonds.nl/nl/boek/1273/het-is-oorlog-maar-niemand-die-het-ziet.

———. “Kabinet Negeert Advies Inlichtingendiensten: Huawei niet Geweerd bij Aanleg 5G-Netwerk” [Parliament Ignores Advice of Intelligence Services: Huawei Not Banned during Construction 5G Network]. de Volkskrant, July 1, 2019. https://www.volkskrant.nl/nieuws-achtergrond/kabinet-negeert-advies-inlichtingendiensten-huawei-niet-geweerd-bij-aanleg-5g-netwerk~b415e11d/.

Munoz, Carlos. “Special Ops Mission Shifts from Terrorism to China, Russia.” *Washington Times*, February 24, 2019. https://www.washingtontimes.com/news/2019/feb/24/special-ops-mission-shifts-terrorism-china-russia/.

Nagtegaal, Bastiaan. “Amerikaanse Ambassadeur vindt Nederlandse Defensie-Investering te Weinig” [American Ambassador Finds the Netherlands Defense Budget too Little]. NRC, May 29, 2019. https://www.nrc.nl/nieuws/2019/05/29/amerikaanse-ambassadeur-vindt-nederlandse-defensie-investering-te-weinig-a3961999.

National Coordinator for Security and Counterterrorism. “Attack in Utrecht and Arrests Confirm Threat,” July 4, 2019. https://english.nctv.nl/latest/news/2019/07/04/attack-in-utrecht-and-arrests-confirm-threat.

———. *Χίμαιρα: An Analysis of the ‘Hybrid Threat’ Phenomenon*. The Hague: Ministry of Justice and Security, 2019. https://english.nctv.nl/documents/publications/2019/09/05/analysis-of-the-’hybrid-threat’-phenomenon.

———. *Cyber Security Assessment Netherlands*. The Hague: Ministry of Justice and Security, 2018. https://english.nctv.nl/binaries/CSBN2018_EN_web_tcm32-346655.pdf.

———. “Duiding Fenomeen Hybride Dreiging” [Explanation of Phenomenon of Hybrid Threat] _tcm31-385687.Pdf. Accessed July 9, 2019. https://www.nctv.nl/binaries/Duiding%20fenomeen%20Hybride%20Dreiging_tcm31-385687.pdf.

Nationaal Coordinator Terrorismebestrijding en Veiligheid. *Cybersecuritybeeld Nederland 2019* [Cybersecurity Picture 2019]. The Hague: Ministerie van Justitie en Veiligheid, 2019. https://www.thehaguesecuritydelta.com/media/com_hsd/report/237/document/CSBN2019-online-tcm31-392768.pdf.

NATO. *AJP 3.20 Allied Joint Doctrine for Cyberspace Operations*. Edition A. Version 1, 3rd Study Draft. NATO, 2019. https://www.nato.int/cps/en/natohq/topics_78170.htm.

———. *Allied Joint Doctrine for Special Operations*. AJP 3.5. Brussels: NATO, 2013. https://standards.globalspec.com/std/1657612/AJP-3.5.

———. “Three Allies Establish Special Forces Command, 07-Jun.-2018.” Accessed August 13, 2019. https://www.nato.int/cps/en/natohq/news_155347.htm.

Nixon, Richard. “The Quotable Richard Nixon.” Richard Nixon Foundation, April 25, 2011. https://www.nixonfoundation.org/2011/04/the-quotable-richard-nixon/.

NRC. “Russische ambassade is spionagecentrum, was betrokken bij poging OPCW binnen te dringen” [Russian embassy is espionage center, and was involved in intended penetration OPCW]. de Volkskrant, December 1, 2018. https://www.volkskrant.nl/nieuws-achtergrond/nrc-russische-ambassade-is-spionagecentrum-was-betrokken-bij-poging-opcw-binnen-te-dringen~bb9402dc/.

Ottis, Rain. “Analysis of the 2007 Cyber Attacks against Estonia.” Cooperative Cyber Defense Center of Excellence. Accessed July 31, 2019. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.

Proper, Ellen. “Too Much Information: Amsterdam Hits Pause on Data-Centre Boom.” Bloomberg, July 15, 2019. https://www.bloomberg.com/news/articles/2019-07-16/too-much-information-amsterdam-hits-pause-on-data-center-boom.

Sanchez, Frank C., Willun Lin, and Kent Korunka. “Applying Irregular Warfare Principles to Cyber Warfare.” *SWJ Blog* (blog), January 29, 2019. https://smallwarsjournal.com/blog/applying-irregular-warfare-principles-cyber-warfare.

Sanger, David E., and Mark Mazzetti. “Israel Struck Syrian Nuclear Project, Analysts Say.” *New York Times*, October 14, 2007, sec. Washington. https://www.nytimes.com/2007/10/14/washington/14weapons.html.

Sanger, David E., and Thom Shanker. “N.S.A. Devises Radio Pathway into Computers.” *New York Times*, January 14, 2014, sec. U.S. https://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html.

Schmid, Markus. “The Concept of Comprehensive Security: A Distinctive Feature of a Shared Security Culture in Europe.” Accessed October 10, 2019. https://apps.dtic.mil/dtic/tr/fulltext/u2/a475775.pdf.

Schmitt, Michael N., ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. New York: Cambridge University Press, 2017.

Simcox, Robin. “The Netherlands’ Luck Is Running Out.” *Foreign Policy*, March 25, 2019. https://foreignpolicy.com/2019/03/25/the-netherlands-luck-is-running-out/.

Singer, P. W. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford; New York: Oxford University Press, 2014.

Spiegel. “The Story of ‘Operation Orchard’: How Israel Destroyed Syria’s Al Kibar Nuclear Reactor” Accessed July 30, 2019. https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html.

Telegraaf. “Rol Nederland bij Speciale Operaties NAVO” [Dutch Role in NATO Special Operations]. June 7, 2018. https://www.telegraaf.nl/nieuws/2142376/rol-nederland-bij-speciale-operaties-navo.

Thomassen, Jacques J. A., Kees Aarts, and Hendrik van der Kolk, eds. *Politieke Veranderingen in Nederland 1971−1998: Kiezers en de Smalle Marges van de Politiek* [Political Changes in the Netherlands 1971−1998: Voters and the Narrow Margins of Politics]. The Hague: SDU Uitgevers, 2000. https://research.utwente.nl/experts/en/publications/13ce06d6-a53e-435e-9a06-4b94942bff82.

Thompson, James D. *Organizations in Action: Social Science Bases of Administrative Theory*. 7th ed. New Brunswick, NJ: Transaction Publishers, 2003.

Trias, Eric D., and Bryan M. Bell. “‘Cyber This, Cyber That . . . So What?’” *Air & Space Power Journal* 24, no. 1 (Spring 2010): 90–100.

Tucker, Patrick. “The CIA Fears the Internet of Things.” Defense One, July 24, 2014. https://www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/.

———. “New Microchip Could Increase Military Intelligence Powers Exponentially.” Defense One, February 4, 2016. https://www.defenseone.com/technology/2016/02/new-microchip-could-increase-military-intelligence-powers-exponentially/125715/.

Turnley, Jessica. *Cross-Cultural Competence and Small Groups: Why SOF Are the Way SOF Are*. JSOU Report 11–1. MacDill Air Force Base, FL: The JSOU Press, 2011. https://www.soc.mil/528th/PDFs/JSOU11-1turnleyF-DWDandSmallGroups(Turnley)_final(16Mar).pdf.

USENIX Enigma Conference. *USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers*, 2016. Video, 0:35. https://www.youtube.com/watch?v=bDJb8WOJYdA.

Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford; New York: Oxford University Press, 2018.

Valeriano, Brandon, and Ryan Maness. “The Fog of Cyberwar: Why the Threat Doesn’t Live Up to the Hype.” *Foreign Affairs*, November 21, 2012. https://www.foreignaffairs.com/articles/2012-11-21/fog-cyberwar.

Votel, Joseph. *Statement of General Joseph L. Votel, U.S. Army Commander Unites States Special Operations Command before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities*. 114th Cong., 1st Sess., 2015. https://docs.house.gov/meetings/AS/AS26/20150318/103157/HMTG-114-AS26-Wstate-VotelUSAJ-20150318.pdf.

Yarger, Harry R. "Towards a Theory of Strategy: Art Lykke and the Army War College Strategy Model." In *Guide to National Security Policy and Strategy*, 2:107–13. Carlisle, PA: U.S. Army War College, 2006. https://catalyst.library.jhu.edu/catalog/bib_2801120.

Yigit, Gorkem, and Dana Cooperson. *From Autonomous to Adaptive: The Next Evolution in Networking*. Analysys Mason. Ciena, 2018. https://www.ciena.com/insights/white-papers/From-Autonomous-to-Adaptive-The-Next-Evolution-in-Networking.html.

Zurhake, Sander. "Special Forces Worden Fundament voor Krijgsmacht" [Special Forces Become Fundament for Armed Forces]. *De Groene Amsterdammer*, November 13, 2015. https://www.groene.nl/artikel/special-forces-worden-fundament-voor-krijgsmacht.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California