Journal of Military and Strategic Studies

VOLUME 16, ISSUE 3 (2015)

# *When The Generation Gap Collides With Military Structure: The Case of Norwegian Cyber Officers*

**Hanne Eggen Røislien**
**Research Professor**
**Norwegian Defence Cyber Academy**

## Introduction

The cyber domain has become acknowledged as both integral and indispensable to military activity.[1] With an inherently military operational aspect, cyber is increasingly viewed as a central part of the military's area of responsibility, be it as a domain for military activity or as a tool that creates new opportunities of action.[2] The pivotal significance of cyber and computer networks to the security of critical infrastructure has contributed to raising awareness about how the comprehension of cyber and cyber security issues necessitates a complex skill-set. This skill-set includes competence within a variety of disciplines, ranging from engineering and computer technology, to law, diplomacy and management.[3] Thus, the inherently inter-disciplinary character of the

[1] See e.g. Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*(New York: Oxford University Press, 2014); Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Journal of Digital Forensic Practice* 3, no. 2-4 (2011).

[2] Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013); Cheryl Pellerin, "For Navy, Cyber Has Inherently Military Operational Aspect,"(American Forces Press Service, June 12, 2013 ).

[3] Ronald Dodge, Costis Toregas, and Lance J. Hoffman, "Cybersecurity Workforce Development Directions," In *Proceedings of the International Symposium on Human Aspects of Information Security & Assurance* University of Plymouth (*HAISA 2012),* pp. 1-12.


ISSN : 1488-559X

cyber domain underscores the recognition that the military necessitates a particular officer type with a multi-disciplinary "cyber competence".[4] Accordingly, gradually more military institutions are recruiting and educating personnel to serve as "cyber officers".

The attributes of the ideal cyber officer, i.e. the ideal skill-set this officer type requires, and how the military most beneficially and efficiently can acquire a professional "cyber officer workforce", is understood very differently by different military institutions and nations. A cyber warrior in a "red team" in the Chinese "Information Security Base" or in the US Cyber Command, operate according to different standards, procedures and practices.[5] This leads to both conceptual confusion and operational challenges. It is consequently a paradox that the cyber officer is a neglected object of study. Focusing on the cyber officers' narratives, this article feeds into the gap in the literature.

In the case of Norway, the Norwegian Defence Cyber Academy (NDCA), starting in 2012, has been given the task to recruit, educate and train individuals in order to provide the Norwegian Armed Forces with an asset that is both capable of conducting operations within the cyber domain as well as operating alongside conventional troops in whatever environment they may find themselves.[6] The NDCA thus has the stated ambition to recruit tech-savvy young men and women with a keen interest in developing their cyber competence within the framework of the military.

Tech-savvy men and women from 'Generation Y', born in the late 1980s or early 1990s, represent an intriguing case and a potential challenge to the military's endeavour to integrate and make use of this generation's competence. They grew up in the post-modern era, recognized not only by its individualism and the erosion of overarching, coherent maxims, but also by the fact that technology is taken for granted. Thus, in the case of the cyber officer a particular generation gap occurs, in which technology and the characteristic of the era collides with the conformity of the military system. Therein lays

[4] Alison D. Miller, *The importance of public-private partnerships in education*, Inroads 4, Issue 4. (2013).
[5] See e.g. p. 3 in Singer and Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*.
[6] Norwegian Defence Cyber Academy, *Study Handbook, 2013-2014, Wing 64 / Wing 65*, Jørstadmoen: Norwegian Cyber Defence competency and Transformation Center [*Studiehåndbok, Forsvarets Ingeniørshøgskole 2013-2014, Ving 64 / Ving 65*, Jørstadmoen: Forsvarets kompetansesenter for kommando og kontroll informasjonssystemer]

a particular challenge. The military must on an institutional level seek solutions as to how to adapt to changes in society and best integrate its recruits, whereas the individual recruits must respond to the role they are placed in and adjust to the system of which they are about to become a part. These two levels conjoin in the generation gap that occurs between recruits and their superiors. It is this generation gap as experienced by the recruits that is the focus of this article.

I will explore this quandary through an examination of cyber officers' testimonies. In particular, the focus is on the cyber officers' conceptualization of "cyber" and how this resonates with that of their superiors'. I will argue that in the case of the cyber officers, friction occurs due to the concurrence of postmodernity, military command structures and cyber. These three factors pull in conflicting directions, and create a peculiar situation as technology and cyber contribute to sharpen the generation gap that necessarily exists between the young generation of cyber officers, and their superiors in the military.

This article is based on ethnographic data derived from interviews with 52 students at the NDCA, 12 of which were in-depth, one-to-one. The remaining students were interviewed in focus groups ranging from four to six students in number. The interviewees were in the age group between 20 and 23. The interviews were semi-structured and focused on questions concerning the cyber officers' conceptualization of the core concepts and areas in their profession, their motivation to serve as cyber officers, and the "human element in combat" (the relevance of cohesion, loyalty to the mission and other core themes in military sociology). The interviews were conducted in 2013-14.

First, I look at previous literature on the cyber officer and situate the article in a theoretical framework based on discussions of how post-modernity influences the context of the cyber officers' ability to perform their profession. Secondly, I proceed to presenting the empirical focus of this article, i.e. the students at the Norwegian Defence Cyber Academy (NDCA). I introduce the case study and proceed to presenting the main findings as identified in the interview data, with reference to the generation gap that occurs. Lastly, I conclude by a discussion about how the "generation gap" identified in the ethnographic data influences not only the ability of the cyber officers to

develop their particular competence within a military framework; I also discuss how cyber competence comprises a particular challenge to military institutions.

**Studying the Cyber Officer**

A great challenge in the study of the cyber officers is the fact that so little research thus far has been done. The multi-disciplinary skill-set required by the cyber officers implies that several different scholarly disciplines potentially conjoin in the study of the cyber officers. Yet, written works tend to follow the same pattern. The available studies are mostly conceptual,[7] with limited little focus on the cyber officers. They are seldom empirical.

For example, while in computer and information sciences there exists conceptual works on how to use technology to enhance situational awareness in different sectors and domains[8], surprisingly few empirical studies are available and only few deal with the military domain. For an emerging literature on cyber situational awareness,[9] the situation seems to be the same. The idea of the "soldier of the future" often seems conjure up a soldier packed with digital equipment.[10]

International law has also grappled extensively with cybersecurity.[11] Key to the discussion is the fact that "Governments, organizations, and commercial interests want people to have access to the Internet and all that it offers but not to be harmed by it."[12] There is thus no lack of law. The question is how to apply it. Ethicists within the "Just

[7] W.D. Hairston et al. Technological areas to improve soldier decisiveness: Insigths from the soldier-system design perspective. Research report ARL-TN-475, U.S. Army Research Laboratory, 2012.
[8] See e.g. J-. Giri et al. *The situation room*. IEEE power & energy magazine, September/October 2012, pp. 24-39; A. W. Eide et al. Inter-organizational collaboration structures during emergency response: A case study. Proc. 10th International ISCRAM Conference, 2013.
[9] S. Jajodia et al. Cauldron. Proc. MILCOM 2011, pp. 1339-1344; S. Jajodia et al. (reds.). *Cyber situational awareness. Issues and research*, Advances in Information Security 46, Springer, 2010.
[10] T. Saarelainen, J. Jormakka. C4I2-Tools for the future battlefield warriors. Proc. 5th International Conference on Digital Telecommunications (ICDT 2010), IEEE, 2010.
[11] J.A Lewis, *Cyberwarfare and its impact on international security*. UNODA occasional papers no.19 (2009); A. Sharma, 'Cyber Wars: A Paradigm Shift from Means to Ends', *Strategic Analysis* 34, no. 1 (2010): pp.62-73; Kristin Bergtora Sandvik, *Towards a militarization of Cyberspace? Cyberwar as an Issue of International Law.* Policy Brief, Peace Research Institute, Oslo, 2012, available at: http://file.prio.no/Publication_files/Prio/Sandvik-Cyberwar-PRIO-Policy-Brief-4-2012.pdf
[12] Mary Ellen O'Connell, "Cyber Security without Cyber War, in *Journal of Conflict & Security Law* (Summer 2012) 17 (2): pp. 187-209. doi: 10.1093/jcsl/krs017, pp. 188.

War" discipline have also started directing their research endeavors to the problem of how to merge cyber warfare with the fundamentals for a just war attack, i.e. proportionality, discrimination, attribution and aggression.[13] Yet, none of these disciplines have explored how the cyber officers apply law and ethics when performing their tasks.

When it comes to the social sciences and humanities, the situation is the same. Research on the cyber officer is limited. The vast literature offering explanations to the "why soldiers fight" question and the 'cohesion' tradition therein, provides one telling example. These numerous studies have contributed to equipping us with rather robust knowledge of critical questions and challenges concerning soldiering. The established knowledge has in turn given practitioners the possibility to make the personnel better prepared and more robust. Yet, the cyber officer is rewarded remarkably little – if any – scholarly attention. At the same time, relevant aspects of the cyber officer's work situation is well-researched. The cyber environment is calling into question fundamental categories of human existence, such as time and space, and changing what it means to be human and how humans are social.[14] At the same time, it is noteworthy that scholars and practitioners for decades have engaged in the study of other officer types. In these studies it has been well-documented that the significance of social and cultural factors for the soldiers' military performance, for their morale and motivation, should not and cannot be underestimated.[15] Rather than being motivated by values or

[13] See e.g. *Cyber War and Cyber Terrorism*, ed. A. Colarik and L. Janczewski, (Hershey, PA: The Idea Group, 2007); the many blogposts by scholar Patrick Linn at Stanford Center for Internet and Society, such as "Could a Cyber Attack be Ethical?" see http://cyberlaw.stanford.edu/about/people/patrick-lin.

[14] See e.g. David Bell, *An introduction to cybercultures* (London: Routledge; Bijker, Wiebe, 2006)." The vulnerability of technological culture" in Helga Nowotny (Ed.), *Cultures of technology and the quest for innovation,* pp.52-69.(New York: Berghahn Books); Cooper, Geoff; Green, Nicola; Murtagh, Ged & Harper, Richard (2002). "Mobile society? Technology, distance and presence" in Steve Woolgar (Ed.), *Virtual society: Technology, cyperbole, reality* (New York: Oxford University Press, 2002), pp. 286-301; Steve Jones, Studying the Net: Intricacies and issues. In Steve Jones (Ed.), *Doing Internet research* (Thousand Oaks, Ca: Sage, 1999), pp.1-27; Daniel Miller and Don Slater, *The Internet: An ethnographic approach* (Oxford: Berg, 2001). Lisa Nakamura, *Cybertypes: Race, Ethnicity, and Identity on the Internet* (London: Routledge, 2002).

[15] Leonard Wong, Thomas A. Kolditz, Raymond A. Millen, and Terrence M. Potter, "Why they Fight: Combat Motivation in the Iraq War.": *Strategic Studies Institute*, (U.S. Army War college, 2003): pp. 1-29.

ethics, soldiers express interpersonal relationships with their primary reference group as the most crucial motivating factor for acting in battle.[16]

The question is, then, whether what we in social sciences "know" about other officer types also holds true for cyber officers. Cyber is already a significant component in the military, and few would disagree with the claim that cyber officers are the "officers of tomorrow". The challenges that the military encounters in the recruitment, education, training and operationalization of these officers must consequently been put under scrutiny. Thus, research combining cyber and soldiering is long overdue.

## The Cyber Officer Profession in Context

The context in which the cyber officer is expected to develop his or her professional character is one in which several fundamental conditions are at odds with each other. It should be well-known to scholars and practitioners of cyber that the question of how to integrate cyber most efficiently and comprehensively into military structures is a complex, ongoing process, and that the recruitment, education and operationalization of cyber officers are equally so. The dynamic and highly flexible character of cyber creates a number of critical challenges as to how cyber should be approached militarily, exemplified by the fact that cyber is itself in rapid development, as well as the temporal character of cyber weapons.[17]

Yet, another key complicating element is of a more generic nature, namely the character of post-modernity. It is widely held that the age we live in is characterized by various degrees of individualization and fragmentation.[18] A challenge in the past few

[16] Edward A. Shils and Morris Janowitz, "Cohesion and Disintegration in the Wehrmacht in World War II," *Public Opinion Quarterly* 12, no. 2 (Summer 1948): pp. 280-315; Leonard Wong, "Combat Motivation in Today's Soldiers." *Armed Forces & Society* 32, no. 4 (2006): pp. 659-663.

[17] Thomas Rid and Peter McBurney, "Cyber-Weapons," *The RUSI Journal* 157, no. 1 (2012).

[18] see Eileen Barker, "The Church without and the God Within: Religiousity and/or Spirituality?," in *The Centrality of Religion in Social Life: Essays in Honour of James A. Beckford*, ed. Eileen Barker(Aldershot & Burlington: Ashgate Publishing Ltd, 2008); James A. Beckford, *Social Theory & Religion* (Cambridge: Cambridge University Press, 2003); Peter Beyer, *Religion and Globalization*(London: SAGE Publications Ltd, 1994); Grace Davie, "Thinking Sociologically About Religion: Contexts, Concepts and Clarifications," in *The Centrality of Religion in Social Life: Essays in Honour of James Beckford*, ed. Eileen Barker (Hampshire & Burlington: Ashgate Publishing Ltd, 2008); Danièle Hervieu-Léger, "Religious Individualism, Modern

decades that has caught the attention in culture studies is "the irresistible progression of individualism and a subjectivization of beliefs and practices which have altered, from top to bottom."[19] As with any paradigm, any attempt at pinpointing the detailed contents is doomed to failure and thus pointless. Thus, as James A. Beckford stated, comprehension of the postmodern paradigm benefits from approaching it as a "catch-all category that loosely covers a bewildering variety of claims about the alleged supersession of modernity by social and cultural conditions, including the erosion of faith in ideological grand narratives, the emancipator power of reason and moral seriousness."[20] In the current context, post-modernity acquires its significance as the "operative terms are pluralism, fragmentation, heterogeneity, deconstruction, permeability, and ambiguity."[21] I consequently concur with Charles C. Moskos et al when they claim that it is "sufficient […] to note that Postmodernism subverts absolute values and introduces a profound relativism into discourse."[22]

Postmodernity presents the military practice and chain of command with a challenge: Within these historical conditions, the needs and aspirations of the military institutional operability, including its hierarchic chain of command, collide with the trends within civil society and face the individual recruits with a glaring contrast. Whereas one in civil society is presented not only with more choices, but also with the encouragement to "pick and choose", the military endeavors to mold its manpower to fit into a system that engenders coherence and unity. The general trends in post-modernity of individualization and the increased spaces for making individual choices may thus prove challenging to the military. Its functionality necessitates that the

Individualism and Self-Fulfilment," in *The Centrality of Religion in Social Life: Essays in Honour of James A. Beckford*, ed. Eileen Barker (Hampshire & Burlington: Ashgate Publishing Ltd., 2008); James A. Beckford, *Religion and Advanced Industrial Society* (London: Unwin-Hyman, 1989).

[19] Hervieu-Léger, "Religious Individualism, Modern Individualism and Self-Fulfilment," p. 30.

[20] Beckford, *Social Theory & Religion*, p. 200.

[21] Charles C. Moskos, John Allen Williams, and David R. Segal, "Armed Forces after the Cold War," in *The Postmodern Military; Armed Forces after the Cold War*, ed. Charles C. Moskos, John Allen Williams, and David R. Segal (New York: Oxford University Press, 2000), p. 8.

[22] Ibid.

soldiers adhere to the military's purpose and mission, and conformity with the military's meaning system is consequently engendered.[23]

On an institutional level, the military has gone through a transition from a modern to a post-modern military. For example, state armies have disassociated themselves from the nation-state and moved from a structural set-up aimed towards fighting invasion wars, towards a more ability-motivated professional military.[24] This transition has also had an impact on the individual soldier, as post-modernity influences the soldiers cognitively. For example, whereas the previous, modern paradigm was one of scholastic learning, the post-modern learning approach and skill acquisition is non-scholastic, emphasising perceptual and emotional involvement, and intuitive and experience-based practice.[25] The challenge is thus two-sided, both in how the military manages to overcome this challenge (cf. the institutional level) as well as how the individual recruits respond to the role they are placed in (cf. the individual level). These two levels meet in the generation gap that occurs between recruits and their superiors.

The term "generation gap" has been coined to describe the differences in cultural and normative attitudes between generations that may cause both friction and misunderstandings.[26] Such a gap may lead to miscommunication across generations. It may also be challenging for professional institutions, as it creates friction between on the one hand, keeping "up to speed" and being dynamic, and, on the other, maintaining continuity, predictability and preserving traditions.

The cyber officers educated at the NDCA today belong to what is popularly called "Generation Y"; the generation born in the late 1980s and early 1990s.[27] In our

[23] Mark J. Osiel, *Obeying Orders: Atrocity, Military Discipline & the Law of War*(New Brunswick and London: Transaction Publishers, 1999).

[24] See e.g. Anders McD Sookermany, "What Is a Skillful Soldier? An Epistemological Foundation for Understanding Military Skill Acquisition in (Post) Modernized Armed Forces," *Armed Forces & Society* 38, no. 4 (2012); Moskos, Williams, and Segal, "Armed Forces after the Cold War."

[25] Sookermany, p. 597.

[26] See e.g. www.investopedia.com

[27] See e.g. Duane F. Alwin, "Generations X, Y and Z: Are They Changing America," *Contexts* 1, no. 4 (November 2002); Ronald Paul Hill, "Managing Cross Generations in the 21st Century: Important Lessons from the Ivory Trenches," *Journal of Management Inquiry* 11, no. 1 (March 2002); Gerry Treuren and

context, two traits of this generation are of particular interest. Firstly, they belong to the first generation "born into" technology. In other words, they did not have to learn to adapt to technology, as it has always been there for the taking. Secondly, they grew up in an era wherein the "Individual human beings are expected to exercise their autonomous judgement in choosing what to believe and how to implement their beliefs in practice."[28] Individuality, independence and flexibility are thus key values to this generation of recruits.

In the generation gap that naturally occurs between Generation Y and the generations above, "the use of computers and the Internet is one area where the generation gap can easily be distinguished."[29] On the most immediate level, use of technology is related to the frequency one uses computers, to competence with regards to different types of software, or how one builds a computer. To Generation Y, cyber has always existed, and the separation between cyber space and physical space is in many regards of little significance as they blend into each other.[30] This is fact also points to the cognitive differences in the users' apprehension of technology, a point I will return to below. Whereas younger generations may "live on the web", the older generations lack trust in the system, and express greater fears of problems like identity theft or fraud.[31]

The cyber officers' generation relate to technology in a way the generation above them cannot ever catch up on.[32] It should also be pointed at that in this situation, the cyber officers "in the making" are at the forefront of their generation. This underscores

Kathryn Anderson, "The Employment Expectations of Different Age Cohorts: Is Generation Y Really That Different?," *Australian Journal of Career Development* 19 (July 2010).

[28] Beckford, *Social Theory & Religion*, 209.

[29] Troy Dunning, "The Generation Gap," *Activities, Adaptation & Aging* 31, no. 2 (2006): p. 73.

[30] Stephen Graham, "The End of Geography or the Explosion of Place? Conceptualizing Space, Place and Information Technology," *Progress in Human Geography* 22, no. 2 (April 1998); Hai Zhuge, "Semantic Linking through Spaces for Cyber-Physical-Socio-Intelligence: A Methodology," *Artificial Intelligence* 175, no. 5-6 (2011).

[31] Dunning, "The Generation Gap."

[32] A. Bhattacherjeea and C. Sanford, "The Intention–Behaviour Gap in Technology Usage: The Moderating Role of Attitude Strength," *Behaviour & Information Technology* 28, no. 4 (2009); Kimberly Severta, Jill Fjelstulb, and Deborah Breiterb, "Information Communication Technologies: Usages and Preferences of Generation Y Students and Meeting Professionals," *Journal of Convention & Event Tourism* 14, no. 2 (2013).

the challenge of the cognitive relation to technology in the generation gap between the cyber officers and their superiors.

Consequently, as men and women in their early 20s enter into military structures, a peculiar situation occurs. A generation accustomed to technology and that takes individual choice and judgement for granted, are expected to adjust to the military's ethos and take orders from their superiors while, at the same time, are expected to excel in their individual competence in a field that is rapidly and constantly changing. As 'tech-savvy', they enter the military with a particular competence that is nurtured, encouraged and needed by the military. At the same time, they will execute their expertise within an institution where rank, authority and decision making largely correspond with age.

In the military, as a rule, the younger you are, the more of an "executor" you are and the more people you have above you from whom you are required to follow orders. This hierarchy is there for a reason. The military necessitates a clear chain of command in order to function and be operational. Few would protest against the principle that climbing the ranks necessitates time-consuming experience within the military system. As professionals in technology, one could hypothesize that the generation gap would be particularly pressing for cyber officers. The cyber officers in this research project are in their 20s and have dealt with technology their whole life, which would place them in quite different category than that of the previous generation, who have had to learn to adjust to technology. This creates a peculiar situation in the military context. The increasing expectation in post-modernity of individuals to exercise their autonomous judgment is counter-intuitive to military functionality. At the same time, key in the generation gap between Generation Y and the generations above, is the relationship with technology.

How do the cyber officers, then, view these challenges? How does the generation gap come into play in their particular field?

**The Case of the Norwegian Defence Cyber Academy**

In Norway, the Norwegian Defence Cyber Academy (NDCA), since 2012, has been integrated into the Norwegian Cyber Defence, wherein the academy is responsible for the education of cyber officers to the Norwegian Armed Forces.[33] Thus, the NDCA attempts to educate and train "cyber officers" from the ground up, educating the students to develop a multi-disciplinary skill-set and to combine cyber competence with an intimate knowledge of the military domain.[34] This includes educating them in information and communication technology and military leadership, while also giving them "knowledge, skills and attitudes in line with the technological and military theoretical development, the values of society, and with international cultural diversity."[35] Accordingly, the recruits embark on a 3.5 year study program with an additional three years[36] of compulsory service in order to become a particular officer type with an expertise in cyber engineering, which at the same time possesses sophisticated military proficiency. They graduate as sergeants with a BA in engineering, in addition to having completed their basic officer training.

The vast bulk of students at the NDCA are between 20 and 24 years of age. Thus, the interviewees in this article were born in the early 1990s and belong to Generation Y. Moreover, they possess the interest in, as well as the potential for, becoming professionals in cyber engineering within a military framework.

The cyber officer is a complex figure, and departs from the popular stereotyped image of tech-savvy geeks who prefer sitting indoors with their candy and soda pop. Rather, these young men and women are physically robust, and it is a prerequisite for recruitment into the education program that they appreciate the hardships of

[33] The academy was established on the basis of the Norwegian Defence University College of Telematics with more than 40 years of experience. The academy currently has an established 3.5 year educational platform producing up to 40 officers within the Command and Control Information Systems (C2IS) and Computer Network Operations (CNO) fields each year.

[34] A similar education model can be found at a few other institutions, such as the US Naval Academy (USNA).

[35] Forsvarets Ingeniørshøgskole [Norwegian Defence Cyber Academy] (FIH/NDCA), "Studiehåndbok, 2013-2014, Ving 64 / Ving 65 [Study Handbook, 2013-2014, Wing 64 / Wing 65]," ed. Cyberforsvarets kompetanse- og transformasjonsavdeling [Norwegian Cyber Defence Competency and Transformation Center] (Jørstadmoen 2013). Translated from Norwegian by author.

[36] The students spend the last six months of the study period in their different departments in the military, while writing their BA thesis. This six-month period is integrated into the three years of compulsory service in the military, making the total time of service 6 years.

soldiering. The cyber officer is stated to be "a robust soldier that participates in the entire spectrum of the [respective] department's tasks and manages complex technology under demanding operative circumstances."[37] The cyber officer is presented to the recruits as the "officer that establishes and controls communication systems and computer systems in the front operative lines and that defends the department against cyber attacks and cyber intelligence."[38]

Obviously, at the core of the cyber officer character lays the concept of cyber, which was a central topic in the interviews where the conceptualization and understanding of the term 'cyber' has been of great concern. How this term is understood is pivotal for what a cyber officer does – and who a cyber officer is. This constitutes an issue of great concern to the cyber officers "in the making." A recurring theme in the interviews was the discrepancy between what the students read into the concept and their superiors take on it. As one interviewee stated:

> Yeah, 'cyber'… I don't get their thinking. I mean, Facebook and Instagram isn't exactly 'cyber', is it? I mean, for real. It certainly isn't what I think it is… But they – I don't know… It means everything and nothing to them, it is so hard to get what they put into that magic box they call 'cyber'. I'd like to follow my own gut feeling, and it keeps telling me that cyber is something else.[39]

As students, recognizing that they are in a learning process, there is an uncertainty amongst the interviewees about which conceptualization of cyber that holds true. In other words, they doubt their own view of what cyber 'is' and question whether they have understood it 'correctly'. At the same time, they hesitate before accepting the conceptualization of cyber that is presented to them. In a focus group the students discussed the conceptualisation of cyber:

> A: They use the term 'cyber' in a way that… they toss it around as if it's some magic powder. As if adding 'cyber' to something makes it more complex or more interesting, when in fact they remove all meaning from the word by doing so. Now 'cyber' means nothing, as I see it.

[37] Ibid.
[38] (FIH/NDCA), "Studiehåndbok, 2013-2014, Ving 64 / Ving 65 [Study Handbook, 2013-2014, Wing 64 / Wing 65]."
[39] Interviewee.

> B: It's just a silly hype, if you ask me. Or make-up. But to them, who have tons of military experience, but just simply lack that same experience with cyber… They can't just keep talking about experience. I mean, you can't just have 'experience' with cyber. It develops so fast. Having all the military expertise in the world doesn't give you cyber competence automatically. They need to trust us on that. Cyber competence is something else, it is something… I don't know how to explain it.
>
> A: Yeah, that's what I meant to say. That it is just a phrase. A word. They use it because it sells. Or what do I know. But they don't use it with reference to its contents, that's for sure. Not most of them. Some perhaps. I mean, there are a few of them [their superiors] who I think know what they talk about, but…[40]

As seen in this example, the students experience a cognitive dissonance in relation to cyber between themselves and their superiors, a dissonance that prevents the students from accepting the conceptualization of cyber that is presented to them. In consequence, they operate with two standards; their own, and that of their superiors. They relate this divergence to their superiors' conceptualization of cyber, on the one hand, and their military superiority, on the other. In other words, they separate cyber competence from military competence. This was stated even clearer by a student as he tried to explain what he saw as his main challenge in his training towards becoming a cyber officer:

> Cyber is a cooler word than communication or network. I mean, not for us. Of course not. But for them, for most of our superiors. For politicians. For – you know, people in charge. And they are generally quite a few years older than us. Of course, they are right: Cyber involves communication. But it also has much more to do with computer networks. But I don't think they care so much about that... I think it is more that it sounds so damned cool. It's a pity, really – that it has that sci-fi 'twang', since it is about so much more than coolness. It is after all about the security of our state, of our people. That's what cyber is about in the military, really. I'd even go as far as saying that it's about survival, although I can hear that it sounds a bit cliché-like. […] So, yes, cyber in the military is really integrated, but it is difficult when they don't get what

[40] Interviewee.

> cyber is really about. I do respect them for their authority, of course I do. Militarily, that is. The green dimension of it. When it comes to cyber… I don't know. I stick to my own judgment mostly.[41]

In this duality of conceptualization, age and the generation gap becomes an explicit factor that accentuates the distance between the generations. It is of little surprise to observe that the cyber officers and their superiors have a radically different relation to cyber and technology. To the young officers, cyber has always existed as easily accessible. This necessarily creates a division between the generations that is first and foremost expressed by the young officers with resignation or simply a shrug, as stated by a 23 year old cyber officer in response to their superiors' long experience with cyber:

> They keep doing that – telling us which year they started doing cyber. They can date the time of their lives when they started doing cyber. They love to do that. 'I've been doing cyber since 1994'. That sort of thing. We can't do that. Of course not. We've been doing cyber since we were born.

The blunt fact that they cannot compete with their superiors when it comes to age is also expressed in a different jargon, ridiculing the generations above them and their need to emphasise how they were "doing cyber" from the cyber domain's early days. The following statement by a student caused much laughter in a focus group among 2nd year students:

> Ha ha ha ha, another story from an elderly who tells me about how he got his first e-mail account…. [in a funny voice:] *I remember my first computer*… ha ha ha.

It was followed by a storm of similar statements in funny voices. Similar sentiments were expressed numerous times, both in one-to-one interviews and in focus groups. The cyber officers swap jokes about everything from the once so hype (but now so dated) commodore computers, about opening email accounts – or rather, not managing to do so – to their superiors' apparent respect for technology. This struggle of the generation above them with defining and conceptualising cyber is a topic of frustration, but also amusement. In a focus group of cyber officer graduates, the students were faced with different attempts at defining cyber. Many caused laughter.

[41] Interviewee.

As one participant said: "I've seen some of the definitions of 'cyber' that is used. 'Electromagnetic field' is my favourite, I think. I mean… seriously?"[42]

The division caused by age is thus fundamental. The simple fact that they have always lived with technology contributes to shaping a cognitively different to cyber that deviates from that of those who have learned how to live with it. Born into technology, they relate to cyber and technology "matter of fact" like. However, for those who have had to learn how to live with technology and cyber, it may not be equally everyday-like. The older the superiors are, the more explicit the difference in relation to technology becomes:

> They have a funny way of approaching 'cyber'. It is like it's with awe or something. As if we're officers from the Matrix. As much as I'd like to be Neo [lead figure in Matrix], I'm actually just a cyber officer. But then again, that doesn't mean that I spend my days on Facebook. Or that I am tinkering with hardware.

As a result, several interviewees have pointed out the problem with developing a common jargon. For example, the superiors can use an expression such as being "a sentinel standing guard":

> But that is rubbish. We don't stand anywhere, we're not on guard. Our *systems* are [on guard]. While we drink coffee. And in a way it is just funny, but in another way – what is actually means… It is scary, since it is not a one-timer. They don't 'happen' to use such expressions. It is all they use.

This comparison to the "old world", to the past, is the last element of significant friction. Comparing cyber to what was "before", makes little if any sense to Generation Y, when "before" equals a time-period they have never experienced. Furthermore, it brings the cognitive dimension of the generation gap to the forefront: The students stressed how their superior officers had a tendency to compare or explain cyber to physical things, such as "imagine wires" or "cyber connects everything together with

[42] Interviewee.

bolts and knots and ropes." Yet, to the students, there is no need to make such comparisons. Cyber is invisible and that is all there is to it.

Such comparisons thus contribute to highlighting the generation gap, accentuating the already existing differences between the generations.

**Towards A Conclusion**

This article proceeded from the quandary about how differences amongst generations come into play in the education and training of cyber officers. Focusing on the cyber officers themselves, the article explored how these young men and women experience how their own views on cyber overlap with the conceptualization of the domain in the military.

Cyber officers are expected to be good at 'doing cyber'. The military invests in them in order to develop an asset from which the military also can benefit. The military needs cyber officer personnel and thus invests in certain individuals. Yet, the individuals recruited belong to a generation that grew up in an era characterized by traits that are at odds with military functionality. More importantly, they have grown up in an era where technology is taken for granted.

The consequence here is that the cyber officers 'in the making' trust their gut feeling more than their superiors, when their superiors' views or narratives are at odds with their own. As seen in the interview data, there is a friction between respect for the system and respect for the competence of the officers. These two are at odds for the cyber officer. While they need both, there is a discrepancy between themselves and their superiors that is so fundamental that it leads to two different comprehensions of cyber. This has two implications for the students. Firstly, in the students' comprehension, the terminology and conceptualization of cyber that they are being taught is literally false. Secondly, they doubt the competence of their superiors when it comes to cyber.

Yet, one should be wary in blaming it all on differences in age and the differences in the generations. As Peter W. Singer and Adam Friedman write: "If it was [solely an issue of age], we could just wait until the old farts died off and all would be solved. Just because someone is young doesn't mean the person automatically has an

understanding of the key issues."[43] Recruits, embarking on a military career, will always be in a squeeze between being 'true' to themselves and adjusting to a system where they will act as representatives of an institution. Recruits will therefore always shoulder a duality and an internal friction between the individual and the collective. As students, the recruits try to rationalize, to adapt, and to understand. They are in a position where learning, internalizing and adjusting is expected from them. Uncertainties in moral and social order both provide possibilities for new worldviews to emerge but may disrupt loyalty, seam lining and hence efficiency.

Accordingly, all militaries face the dilemma of how to rework the ethos of prior socialization and find a balance between being dynamic and "up to date" and at the same time maintaining continuity and predictability. Thus, turning recruits into soldiers includes the reformation of ethical, social and cultural consciousness, wherein the recruits internalize the military's collective meaning system, therein the chain of command. The military, therefore, must to some degree stage and foster coherence amongst its recruits, and counteract trends in civil society.

For that reason, the interviewees articulated their attempts at rationalizing the difference in both jargon and comprehension of cyber. It is noteworthy that in this rationalization, the students express a duality that reflects the two aspects of the cyber officer, namely the military and the technological. That is to say, the students expressed their concern on how to make these concepts balance.

It is not surprising that there exists a generation gap between young men and women in their 20s and their superior officers when it comes to everything from jargon, comprehension of the profession as well as the use of technology. However, when it comes to cyber and the operationalization of cyber within the military context, these differences have a more fundamental implication. The young cyber officers and their superiors are not necessarily talking about the same, nor are they dealing with the same issues.

Because cyber is viewed in such diverging terms, it raises the question of not only what cyber is, but also the military's ability to operate in the cyber domain. The discrepancy can to some degree be related to the inherently inter-disciplinary character

[43] Singer and Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, p. 5.

of cyber, and cyber feeds into all aspects of the military. Consequently, scholars argue that it creates a misconception when cyber is described as a "domain." Rather, cyber ought to be considered a "substrate." Today, all levels of war are 'cybered', as are all types of conflict and all phases of military operations.[44] It is consequently unfeasible to single it out as a separate area of concern. Approaching cyber as a substrate rather than as a domain underscores the recognition that the military necessitates a particular officer type with a multi-disciplinary "cyber skill-set".[45]

When adding postmodernity as a factor in the professional context of the cyber officers, one should be cautious and point out that this does not mean that this article implies an attempt to identify postmodern traits of the Norwegian armed forces, nor does it imply the application of a postmodern or poststructuralist analysis.[46] Rather, adding postmodernity as a factor directs attention to the framework and conditions for the generation gap that exists between the young cyber officers and their superior officers. It cannot be ignored that the recruits entering the military today do so having learned their basic skills in society in a historical context that focuses on the individual, and therein on individual freedom, choice and independence. Expanding on this line of argument, Anders McD Sookermany has afforded the postmodern soldier much scholarly attention. He argues that today, individual judgement is becoming increasingly important, as is the soldier's ability to respond to context, and to "display initiative, flexibility and independence."[47] In practice, this implies that the cyber officers are expected to be trustworthy, professional and to be able to make their own analysis and operate in accordance with it, all traits in line with the dominating paradigm of post-modernity.

Integrating cyber into military structures is as challenging as it is necessary. Though while scholars disagree as to whether "cyber war" is a contradiction in terms[48]

[44] Peter Dombrowski and Chris C. Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," *Naval War College Review* 67, no. 2 (2014).
[45] Alison D. Miller, "The importance of public-private partnerships in education," *Inroads* 4, no. 4 (2013).
[46] These two approaches are in polemic with the approaches coined by Harry Bondy in his article "Postmodernism and the Source of Military Strength in the Anglo West" in *Armed Forces & Society* 31 (Fall 2004): pp. 31-61.
[47] Sookermany, pp 593, 597
[48] The polemic discussion between Thomas Rid on the one hand, forwarded in his book "Cyber War Will Not Take Place", and Richard A. Clarke, on the other, prove a telling example. See Rid, *Cyber War Will*

or on how cyber should or could be defined as a meaningful term, there is a general consensus that the cyber domain should be part of the military's AOR. Cyber has "an inherently military operational aspect."[49] The complexity of the cyber domain poses a particular challenge to the military, as it pervades all sectors and is at the same time lacking coherent and comprehensive guidelines.[50] The fact that it is "surely not an exaggeration to assert that every aspect of general principles of international law is disputed"[51] complicates matters further.

One interviewee summarized this quandary quite precisely when he said the following:

> They [their superior officers] can be wise and skilled and experienced in so many ways. But they are too used to the old, too used to how things were before. So they always try to adjust the new to the old, read the new in light of what is no longer valid. They always try to make the new fit in the old patterns. But it doesn't make sense. They are stuck in thinking in hours or in physical stuff. When it is about seconds, nano-seconds even. Or about all the stuff we cannot see.

Maybe this is what it is all about - Looking ahead or looking back.

*Not Take Place*; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, vol. New York (Ecco, 2010).

[49] Pellerin, "For Navy, Cyber Has Inherently Military Operational Aspect."

[50] Accordingly, Dombrowski and Demchak argue that cyber is in fact not a domain, but a substrate, as it is "an underlying layer on which modern society is built." Dombrowski and Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain."

[51] Katharina Ziolkowski, "General Principles of International Law as Applicable in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, ed. Katharina Ziolkowski(Tallinn: NATO CCD COE Publication, 2013): p. 137.

Bibliography

(FIH/NDCA), Forsvarets Ingeniørshøgskole [Norwegian Defence Cyber Academy]. "Studiehåndbok, 2013-2014, Ving 64 / Ving 65 [Study Handbook, 2013-2014, Wing 64 / Wing 65]." edited by Cyberforsvarets kompetanse- og transformasjonsavdeling [Norwegian Cyber Defence Competency and Transformation Center]. Jørstadmoen, 2013.

Alwin, Duane F. "Generations X, Y and Z: Are They Changing America." *Contexts* 1, no. 4 (November 2002): pp. 42-51.

Barker, Eileen. "The Church without and the God Within: Religiousity and/or Spirituality?". In *The Centrality of Religion in Social Life: Essays in Honour of James A. Beckford*, edited by Eileen Barker, 187. Aldershot & Burlington: Ashgate Publishing Ltd, 2008.

Beckford, James A. *Religion and Advanced Industrial Society*. London: Unwin-Hyman, 1989.

———. *Social Theory & Religion*. Cambridge: Cambridge University Press, 2003.

Beyer, Peter. *Religion and Globalization*. London: SAGE Publications Ltd, 1994.

Bhattacherjeea, A. , and C. Sanford. "The Intention–Behaviour Gap in Technology Usage: The Moderating Role of Attitude Strength." *Behaviour & Information Technology* 28, no. 4 (2009): pp. 389-401.

Clarke, Richard A., and Robert K. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*. Vol. New York: Ecco, 2010.

Davie, Grace. "Thinking Sociologically About Religion: Contexts, Concepts and Clarifications." In *The Centrality of Religion in Social Life: Essays in Honour of James Beckford*, edited by Eileen Barker, pp. 15-28. Hampshire & Burlington: Ashgate Publishing Ltd, 2008.

Dombrowski, Peter, and Chris C. Demchak. "Cyber War, Cybered Conflict, and the Maritime Domain." *Naval War College Review* 67, no. 2 (2014): pp. 71-96.

Dunning, Troy. "The Generation Gap." *Activities, Adaptation & Aging* 31, no. 2 (2006): pp. 73-75.

Geers, Kenneth. "The Cyber Threat to National Critical Infrastructures: Beyond Theory." *Journal of Digital Forensic Practice* 3, no. 2-4 (2011): pp. 124-30.

Graham, Stephen. "The End of Geography or the Explosion of Place? Conceptualizing Space, Place and Information Technology." *Progress in Human Geography* 22, no. 2 (April 1998): pp. 165-85.

Hervieu-Léger, Danièle. "Religious Individualism, Modern Individualism and Self-Fulfilment." In *The Centrality of Religion in Social Life: Essays in Honour of James A. Beckford*, edited by Eileen Barker, pp. 29-40. Hampshire & Burlington: Ashgate Publishing Ltd., 2008.

Hill, Ronald Paul. "Managing Cross Generations in the 21st Century: Important Lessons from the Ivory Trenches." *Journal of Management Inquiry* 11, no. 1 (March 2002): pp. 60-66.

Moskos, Charles C., John Allen Williams, and David R. Segal. "Armed Forces after the Cold War." In *The Postmodern Military; Armed Forces after the Cold War*, edited by Charles C. Moskos, John Allen Williams and David R. Segal, pp. 1-13. New York: Oxford University Press, 2000.

Osiel, Mark J. *Obeying Orders: Atrocity, Military Discipline & the Law of War*. New Brunswick and London: Transaction Publishers, 1999.

Pellerin, Cheryl. "For Navy, Cyber Has Inherently Military Operational Aspect." *American Forces Press Service*, June 12, 2013

Rid, Thomas. *Cyber War Will Not Take Place*. London: Hurst & Company, 2013.

Rid, Thomas, and Peter McBurney. "Cyber-Weapons." *The RUSI Journal* 157, no. 1 (2012): pp. 6-13.

Severta, Kimberly, Jill Fjelstulb, and Deborah Breiterb. "Information Communication Technologies: Usages and Preferences of Generation Y Students and Meeting Professionals." *Journal of Convention & Event Tourism* 14, no. 2 (2013): pp. 124-43.

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

Sookermany, Anders McD. "What Is a Skillful Soldier? An Epistemological Foundation for Understanding Military Skill Acquisition in (Post) Modernized Armed Forces." *Armed Forces & Society* 38, no. 4 (2012): pp. 582-603.

Treuren, Gerry, and Kathryn Anderson. "The Employment Expectations of Different Age Cohorts: Is Generation Y Really That Different?". *Austrational Journal of Career Cevelopment* July, 19 (2010): pp. 49-61.

Zhuge, Hai. "Semantic Linking through Spaces for Cyber-Physical-Socio-Intelligence: A Methodology." *Artificial Intelligence* 175, no. 5-6 (2011): pp. 988-1019, Special Review Issue.

Ziolkowski, Katharina. "General Principles of International Law as Applicable in Cyberspace." In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski. Tallinn: NATO CCD COE Publication, 2013.