Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations

Maathuis, Clara; Pieters, Wolter; Van Den Berg, Jan

DOI
10.1109/MILCOM.2018.8599729

Publication date
2019

Document Version
Final published version

Published in
2018 IEEE Military Communications Conference, MILCOM 2018

Assessment Methodology for Collateral Damage and Military (Dis)Advantage in Cyber Operations

Clara Maathuis
Delft University of Technology
TNO, Netherlands Defense Academy
Netherlands
clara.maathuis@tudelft.nl

Wolter Pieters
Delft University of Technology
Delft, Netherlands
w.pieters@tudelft.nl

Jan van den Berg
Delft University of Technology
Delft, Netherlands
j.vandenberg@tudelft.nl

***Abstract*—Cyber Operations stopped being utopia or Sci-Fi based scenarios: they became reality. When planning and conducting them, military actors encounter difficulties since they lack methodologies and models that support their actions and assess their effects. To address these issues by tackling the underlying scientific and practical gap, this article proposes an assessment methodology for the intended and unintended effects of Cyber Operations, labeled as Military Advantage, Collateral Damage and Military Disadvantage, and aims at supporting the targeting process when engaging targets in Cyber Operations. To arrive at this methodology, an extensive review on literature, military doctrine and methodologies was conducted combined with two series of interviews with military commanders and field work in joint military exercises. The assessment methodology is proposed considering multidimensional factors, phases and steps in a technical – military approach. For validation, one realistic Cyber Operation case study was conducted in a focus group with nine military experts plus four face-to-face meetings with another four military experts.**

Keywords—cyber operations, cyber warfare, cyber weapons, targeting, collateral damage, military advantage, effects assessment.

I. Introduction

"War is never an isolated act…in war the result is never final." (Clausewitz, On war)

Compared with other warfare domains, cyberspace is geographically less constrained [1] as it is a dynamic and fast changing environment where "new nodes are discovered and a kaleidoscope of network patterns occurs and disappears" [2]. Since Cyber Operations can amplify or support other Military Operations [3], they embed the power to influence or threaten to influence enemies [4] by efficiently and effectively engaging targets with proper cyber weapons/capabilities. When assessing, predicting or estimating the effects of Cyber Operations, one needs to "think the unthinkable" [5] since this is very difficult [4, 6] considering data reliability and accuracy. Different methodologies and mechanisms are used to (partially) solve these issues in kinetic Military Operations, but for Cyber Operations they are inexistent in the field and scarcely tackled in the academic literature.

Addressing these issues combined with the growing number of Cyber Operations globally conducted (e.g. Georgia, Stuxnet, Ukraine), this article aims at designing an assessment methodology for the intended and unintended effects (Military Advantage, Collateral Damage and Military Disadvantage) that supports military commanders and their staff (e.g. intelligence and execution) when targeting in Cyber Operations. In this research, the following definitions were considered [7]:

a) Military Advantage as intended effects that contribute to achieving military objectives.

b) Collateral Damage as unintended effects that do not contribute to achieving military objectives, but impact civilian assets, in the form of civilian injury or loss of life and/or damage or destruction to civilian objects and/or environment.

c) Military Disadvantage as unintended effects that do not contribute to achieving military objectives and impact allies, friendly, neutral, even the target or conducting actors.

A multidisciplinary research was carried out in the fields of cyber warfare/security and military, based on reviewing academic literature and military doctrine, military methodologies and mechanisms. Additionally, two sets of interviews with eighteen military commanders were conducted plus field work in joint military exercises. Since traditional approaches are less applicable to Cyber Operations (e.g. collateral damage estimation) [8], the abovementioned resources allowed the design of this methodology. To validate, two virtual Cyber Operations case studies were conducted, but due to space limitations, only one of them is presented in this article. The validation was done in two steps: first, in a focus group organized with nine military experts, and second, in four face-to-face meetings with another four military experts.

The remainder of this article is structured as follows. The second section summarises relevant research. The third section presents the research approach pursued by this article. The fourth section introduces the assessment methodology. The fifth section presents the Cyber Operation case study on which this methodology was validated and the validation results. The last section discusses contributions and future work.

II. Related Work

[9] provides guidance to conducting Military Operations by EU forces and discusses necessary requirements and steps for avoiding or at least minimizing Collateral Damage. This view is aligned with the one enclosed in the methodology used by

978-1-5386-7185-6/18/$31.00

NATO and US [10, 11] and implies the following levels of assessment: i) target validation and initial CDE (Collateral Damage Estimation) analysis, ii) general and target size analysis overview, iii) weaponeering analysis overview, iv) refined analysis overview, and v) casualty analysis overview. Control measures for avoiding or minimizing the unintended effects in Cyber Operations and a multi-level / phase perspective are likewise incorporated in this research.

A methodology for assessing collateral damage for nonfragmenting Precision-Guided Weapons was designed by [11] considering as lethality scale: lethal, severe, moderate, light and no injury. The severity scale used by U.S. DoD is: deceased (lethal), very serious, serious, incapacitated and not serious injured [12]. Both scales are integrated in this research.

[13] analyses tools used to assess Collateral Damage in Operations Allied Force, Enduring Freedom and Iraqi Freedom, and argues that collateral damage estimation methodologies need to be accurate, responsive and human-factored by providing graphics that facilitate decisions. Aligned with [9, 10], this research uses different tables to support the assessment process and decision making.

[14] proposes the following design considerations when assessing the impact of a cyber incident: focus on information, information asset valuation, knowledge retention, mission representation and mission impact estimation, and secure notification. Due to their generality and applicability, these considerations were presumed when designing the assessment methodology that this research introduces. Additionally, an effective cyber damage assessment is based on identifying and valuating assets considering how they are vulnerable, presented in a structured and documented way. Accordingly, each phase of the assessment methodology proposed in this research is structured, documented and sequentially introduced.

[15] conducts a cyber security assessment for tactical C2 evaluated on case studies, in a similar way that the evaluation is done in the present research.

III. Research Methodology

This research aims at designing an effects assessment methodology for targeting in Cyber Operations. This requires a multidisciplinary perspective by combining multiple methods of research from cyber and military domains. Accordingly, a design science approach [16] is considered since it allows artefacts (i.e. frameworks, methods, models) to be designed and evaluated systematically based on the following activities:

Activity I: Problem Identification and Motivation

The motivation underlying this research is twofold. First, Cyber Operations have the potential to becoming a key component of Military Operations, however they lack dedicated methodologies for planning and execution, and this impacts military and civilian actors, and society itself. On this ground, two sets of structured and focused interviews [16] with eighteen military commanders (eight in the first set and ten in the second) with significant international experience, from Netherlands, Germany and U.S. were held in 2016 and 2017. The military experts were asked to elaborate on their requirements and expectations regarding assessing Collateral Damage and Military Advantage in Cyber Operations. Moreover, they were questioned regarding the possibility of not receiving the expected information and asked how they would react in such a case. Furthermore, field work was carried out in 2016 and 2017 by direct participating and observing in two joint military exercises [17] that contributed to achieving a comprehensive vision on Cyber Operations and considerations for assessing their effects. Secondly, from an extensive review of scientific literature, military doctrine and reports, general approaches for effects or impact assessment have been considered (in Related Work section) or focused on limiting or controlling Collateral Damage [18], but lack methodologies for assessing Collateral Damage, Military Advantage and Military Disadvantage in Cyber Operations.

From the abovementioned resources, the following requirements were established for designing the effects assessment methodology in Cyber Operations:

a) To be structured, adaptable and illustrative.

b) To be compatible, familiar or designed in a similar way as the methodologies used in kinetic Military Operations.

c) To consider time, space and force dimensions.

d) To be evaluated on realistic Cyber Operations scenarios.

Activity II: Solutions Objectives

Furthermore, the objectives of this research are:

- To identify the dimensions and factors that can be used to assess Collateral Damage, Military Advantage and Military Disadvantage when targeting in Cyber Operations.
- To design an assessment methodology for Collateral Damage, Military Advantage and Military Disadvantage when targeting in Cyber Operations.

Activity III: Design and Development

The functionality and architecture of the assessment methodology (artefact) are determined, and based on all gathered resources, the design is executed following the requirements defined in *Activity I.*

Activity IV: Demonstration

To demonstrate through experimentation or case study, two face-to-face meetings with two military experts were individually organized in 2017. The first meeting was a brainstorming session regarding the development of virtual and realistic case studies that would be suitable to evaluate the proposed methodology. In the second meeting, two alternatives for two case studies were proposed to the experts, and for each case study they advised to choose one. In this article, due to space limitations, only the first case study is presented.

Activity V: Evaluation

The assessment methodology designed in *Activity III* is evaluated on a case developed in *Activity IV* in two phases. In the first phase, in a focus group [31] organized by TNO (the Netherlands Organization for Applied Scientific Research) and the Netherlands MoD in one day in June 2017 under the name "Effects Assessment and Targeting Decisions in Cyber Warfare". Nine experts were selected and invited to participate based on their background and experience. In the second phase, in four face-to-face meetings organized between June – October 2017 with another four military experts to refine this methodology. Finally, the methodology is proposed.

Activity VI: Communication

The results of this research are communicated through meetings, e-mails and the present article.

IV. DESIGN OF ASSESSMENT METHODOLOGY

The effects assessment in Cyber Operations methodology was designed based on the requirements and considerations previously presented, and aims at assessing effects prior to engaging targets in Cyber Operations. However, it can also be used after engaging targets as guidance when analysing effects. The military experts interviewed and [7, 3, 19] argue that an integration of spatial (spreading), temporal (duration) and force (severity) factors, together with probabilities needs to be considered. Force is expressed by the type of effects. Hence, these factors are presented in Table I – III and further used:

TABLE I. SPATIAL SCALE FACTORS (SPREADING)

Target (T)	Network of Target (NT)	National (N)	Regional (R)	Global (G)

TABLE II. TEMPORAL SCALE FACTORS (DURATION)

Short Term (ST)	Medium Term (MT)	Long Term (LT)
0 – 1h 1h – 1 day	1 day – 1 week 1 week – 1 month	1 month – 6 months 6 months – 1 year 1 year – 3 years

TABLE III. PROBABILITY

Probability	Value
No (N)	0%
Low (L)	0 – 25%
Moderate (M)	25 – 50%
High (H)	50 – 75%
Very high (VH)	75 – 100%

The proposed methodology is structured in five phases compatible with the current methodologies used in kinetic Military Operations [10, 11], as follows: Phase I. Target Identification and Validation, Phase II. Target Analysis, Phase III. Target Effects Assessment, Phase IV. Collateral Effects Assessment and Phase V. Minimization of Unintended Effects. Furthermore, each phase is elaborated:

Phase I: Target Identification and Validation

In this phase, entities that allow to (threaten to) influence adversaries and achieve military objectives are identified and validated as targets. This phase is similar to the first level of assessment applicable to kinetic Military Operations [10, 11]. Therefore, the necessary information needs to be considered as illustrated in the next two steps.

Step I: Target Identification

To identify targets the next information is needed: name, category, set, type, description, function, geolocation, surroundings, environment, defense mechanism, vulnerability, sensitivity, priority, engagement timestamp and status [19]-[22].

Step II: Target Validation

To be validated as a target, an entity should be a lawful military target considering the criteria provided by LOAC [26]: nature, location, purpose or use. If this entity is not positive identified (PID), then it cannot be engaged [24] and other options should be considered for engagement or the operation should be suspended or cancelled.

Phase II: Target Analysis

In this phase, sufficient information about the target should be acquired to be engageable in a Cyber Operation. From this phase, the assessment is tailored to the cyber context. Hence, necessary information useful to analyse it should be considered regarding its system, hardware and software architectures and elements included, as illustrated in the layered model depicted in Fig. 1 and described in the next steps:

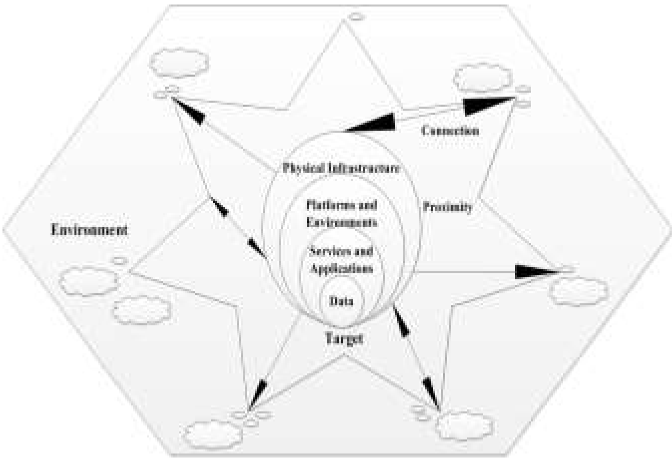

Fig. 1. Target Analysis Model

Step II.I: System Architecture

Step II.I.I: Structure, components, functions and behaviour

Information about the system structure, components, their functions and behaviour is required [19]-[21].

Step II.I.II: Connections, dependencies and connectivity

Information about the network topology, traffic, connections and dependencies [25]-[27] as well as type, status and operator / provider of connectivity have to be known.

Step II.II: Hardware Architecture

Information about the physical infrastructure, devices (e.g network devices like routers or switches, different sensors), their functionality, status, defense mechanisms (e.g. locks, encryption), protocols and vulnerabilities (hardware or configuration) should be acquired.

Step II.III: Software Architecture

Information about the software infrastructure, applications (e.g. firmware, middleware, desktop, web or mobile), protocols and data together with their functionality, status, defense mechanisms (e.g. encryption, firewalls, IDS/IES, VPN) and vulnerabilities (software or configuration) should be gained.

Phase III: Target Effects Assessment

The intended and unintended effects of Cyber Operations are assessed using of the factors introduced by Table I – III.

Step III.I: Military Advantage Assessment

The interviewed military experts stressed that currently Military Advantage is assessed by military commanders and their staff based on feeling, background, experience, common sense using the information about the target, without relying on a specific assessment methodology. Furthermore, Military Advantage should be assessed on all warfare levels as well as in other warfare domains since cyberspace is a cross-domain of warfare [19], as Tables IV and V portray:

TABLE IV. MILITARY ADVANTAGE ON EACH LEVEL OF WARFARE

Battlefield / Level	Strategic	Operational	Tactical
Land / Sea / Air / Space / Cyber			

TABLE V. MILITARY (DIS)ADVANTAGE IN CYBER OPERATIONS

Type	On Target	Duration	Spreading	Severity	Probability

In Table V, '*Type*' represents the type of Military Advantage, such as communication delay or target neutralization. '*On Target*' means combatants, military logic / virtual objects and military physical objects as military targets.

Step III.II: Efficiency, effectiveness and performance

Indicators regarding the efficiency, effectiveness (MoE) and performance (MoP) [20] in achieving military objectives in Cyber Operations are useful since the effects assessment process is a continuous and adaptive process. This is indicated in Table VI.

TABLE VI. EFFICIENCY, EFFECTIVENESS AND PERFORMANCE IN CYBER OPERATIONS

Name Indicator	Level Of
Efficiency	Low
Effectiveness	Medium
Performance	High

Phase IV: Collateral Effects Assessment

Cyber Operations have a wide range of effects [25] that can impact the target as well as other actors, military or civilian in the sense of allies, friendly, neutral or even conducting actors. Moreover, each category of collateral effects is elaborated.

Step IV.I: Collateral Damage Assessment

In Table VII, '*Type*' means the type of Collateral Damage, such as injury of people or communications delay. '*On Asset*' represents non-combatants, civilian logic / virtual objects and civilian physical objects that are forbidden to target.

TABLE VII. COLLATERAL DAMAGE IN CYBER OPERATIONS

Type	On Asset	Duration	Spreading	Severity	Probability

A significant role in deciding if a target can be engaged in a Cyber Operation plays the proportionality test, which stresses that Collateral Damage should not be excessive in relation to Military Advantage [29]. That being said, Collateral Damage is considered either: i) Not Accepted, ii) Tolerated, iii) Accepted.

Step IV.II: Military Disadvantage Assessment

Table V applies also for assessing Military Disadvantage. Military Disadvantage impacts allies, friendly, neutral or even the target or conducting actors. '*Type*' can be for example communications perturbation or operational instability.

Phase V: Minimization of Unintended Effects (Collateral Damage and Military Disadvantage)

In this phase, control measures for avoiding or minimizing Collateral Damage and Military Disadvantage are proposed:

Step V.I: Minimization of Collateral Damage

Step V.II: Minimization of Military Disadvantage

To avoid or minimize Collateral Damage and Military Disadvantage, control measures regarding a better situational awareness, correct, accurate, multi-source and last minute (up to date) intelligence are necessary. Furthermore, high accuracy and precision regarding engaging the right target in the most specific way by using efficient, effective and desirably adaptive and intelligent cyber weapons/capabilities are decisive. These measures should be considered from the design phase to be optimal. Moreover, control measures regarding engaging the target with a different cyber weapon or a different engagement method should also be included. Additionally, if all control measures are considered ineffective, another target should be nominated or the operation should be suspended or cancelled.

VI. VALIDATION: CYBER OPERATION CASE STUDY

A case study was designed from scratch and prepared between January to May 2017 respecting the last requirement concerning the design of an assessment methodology, the advices that military commanders provided and current global security issues. This case study was virtually conducted, is depicted in Fig. 2, and was used to validate the proposed methodology with military experts, in a double process: first, in a focus group, and second, in four face-to-face meetings. The experts were asked 13 questions structured in five groups: opening, introductory, transition, key and ending questions.

Hence, following the context description proposed by [7] for representing and simulating Cyber Operations, the following information was used to evaluate Phases I and II of the methodology: Context, Actor, Type, Military Objective, Target, Cyber Weapon and Geolocation, as follows:

Context: A crisis in Risian evolved into an international armed conflict due to humanitarian concerns, terrorist groups support that impacted Risian's population, neighbour countries and escalated internationally. Amdasia supported by other states decided to launch a ballistic missile attack on Risian's military land HQ in Risian's capital. Recently, Risian invested in its missile program. Its Ballistic Missile Defense System which is a land-based system that can detect, track, engage and destroy short and medium range ballistic missiles, is procured from Limia (a neutral country and ally to Amdasia).

Actor: Risian, Amdasia, Limia.

Type: Offensive Cyber Operation.

Military Objective (for Amdasia): to prevent the surface-to-air anti-ballistic missile of Risian to reach its target – the surface-to-surface ballistic missile launched by Amdasia against the military land HQ located in Risian's capital.

Target: the anti-ballistic missile of Risian (see 4 in Fig. 2) fired from the missile squadron located at the military base at 100 km distance to the capital of Risian that is a part of Risian's Ballistic Missile Defense System.

Fig. 2. Ballistic Missile Defense Cyber Operation

Legend: 1. Communications satellite, 2. Surveillance satellite (early warning), 3. Ballistic Missile Defense System (BMDS) Ground Base, 4. BMD Interceptor/Launcher, 5. BMD C2, 6. Another BMDS Ground Base, 7. Another BMD Interceptor/Launcher, 8. BMDS radar, 9. BMDS Ground Base, 10. BM Launcher, 11. BM at the beginning of the mid-course phase, 12. BM trajectory, 13. Calculated collision point between the BM and the anti-BM, 14. Capital of Risian, 15. Civilian airport, 16. Air Force military base.

Cyber Weapon: Risian subcontracted a software development company from Limia to develop the software that its Ballistic Missile Defense Command and Control uses. Amdasia is a step ahead of Risian considering possible counterattacks in case of launching ballistic missiles against Risian. That is why a Senior Software Engineer (insider) was infiltrated in the design and development phases of Risian's software at the software company. This allowed the introduction of a software vulnerability of which exploit will automatically be activated in special geostrategic conditions when a ballistic missile from Amdasia is detected. If Amdasia launches its ballistic missile, preparations are made by Risian to launch an anti-ballistic missile against it. As this happens, the anti-ballistic missile self-destroys in the boost phase and explodes in the neighbourhood, probably at the periphery of Risian's capital. Therefore, Amdasia's ballistic missile follows its ballistic flight to deliver its warhead and impact its target.

Tables VIII and IX present the results from evaluating Phase III of the proposed methodology. Regarding efficiency, effectiveness and performance in achieving the military objective, this Cyber Operation was considered by the military experts as being High or between Medium to High.

TABLE VIII. MILITARY ADVANTAGE IN CASE STUDY ON WAR LEVELS

Battlefield / Level	Strategic	Operational	Tactical
Land	Limit Risian's ability to C2. Military objective is achieved.	Damage or destruction of Risian's land HQ. Disruption of Risian BMDS.	Limit Risian's means to receive orders and C2.
Sea	No / Possible option.	NAK	NAK
Air	Influence or limit Risian's response. Limit Risian's defensive reaction in air & space.	Limit Risian's ability to C2 operations and to use anti-BM in near-future air&space operations. Limit or alter the order to process information.	Limit Risian's means and ability to receive orders and information through the C2.
Space			
Cyber	Attribution. Cyber as a real offensive option and general awareness. Limit / Influence Risian's cyber defense capability. Risian's systems and C2 exposure, compromise.	Influence / Allowing future exploitation of Risian's sytems and operations. Limit or destroy Risian's ability Risian to C2 operations.	Reducing the BMD functionality and capability. Control of Risian's C2 systems.

TABLE IX. MILITARY ADVANTAGE IN CASE STUDY

Type	On Target	Duration	Spreading	Severity	Probability
Limit effectivity	BMD C2	ST-MT	T,NT or N	Disruption and Control	H–VH
			R or G.		L
	anti-BM	ST	T	Destruction	VH
Influence	Risian	MT-LT	N or R	Influence power balance	H
Limit	Combatants	ST-MT	N or R	Limit physical force	H
Disruption and Control	BMD C2	ST-MT	T,NT and N	Disruption and Control	H

Tables X and XI present the results from evaluating Phase IV. Kinetic effects are produced by the fired missiles. Experts considered Collateral Damage as being Accepted or Tolerated.

TABLE X. COLLATERAL DAMAGE IN CASE STUDY

Type	On Asset	Duration	Spreading	Severity	Probability
Injury or Loss of life	Civilians	ST-MT	Capital area	Injury or Death	L-M
Mental / Psychologic	Civilians	MT-LT	Capital area or N	Mental injury	M
Damage or destruction	Civilian Critical Infrastructure	ST	N	Damage or destruction	L-M
Infection	Civilian systems and services	ST-MT	N or G	Infection	L
Alteration or destruction	Civilian data	ST-MT	N, R or G	Alteration or destruction	L
Damage or destruction	Environment	ST-MT	N or R	Damage or destruction	L-M

TABLE XI. MILITARY DISADVANTAGE IN CASE STUDY

Type	On Target	Duration	Spreading	Severity	Probability
Risian and Limia (if attributed)	Between Risian and Limia	NAK	R or G	Tensions / Conflict	M-H
Distrust BMD C2	Limia or Risian	ST-MT	T	Distrust	M-H
Failure (if C2 is updated)	Cyber Operation on Risian's BMD C2.	ST	T or NT	Failure	H-VH
Detection	Cyber Weapon	ST	T	Detection	L

Type	On Target	Duration	Spreading	Severity	Probability
Spreading and Infection	Limia, allies, friendly or neutral actors	ST-MT	R or G	Infection or disruption	L-M
Instability	Amdasia,allies, friendly or neutral actors	ST-MT	G	Instability	L
Re-use	BMD C2	All	T	Re-use	L

When evaluating phase V, the experts advised to engage this target since Collateral Damage was not expected excessive in relation to Military Advantage. In unanimity, they decided that if insufficient information is given, the target should not be considered for engagement, and stressed that "civilian lives are the most precious and most important". Aligned with [15, 30], this research gradually assesses the effects of Cyber Operations to anticipate possible futures and validates it by bringing "the researcher into direct contact with the potential users of the artefact" [31] and with domain experts by considering suitability, feasibility, acceptability and completeness as evaluation criteria [31]. Based on these results, the methodology fulfilled the requirements, reflects its effectiveness and applicability, and provided meaningful insight into the dynamics of targeting in Cyber Operations.

VII. Conclusions

Since the dawn of history wars were a part of the human existence and experience [32]. By expanding the theatre of operations in the cyber domain, we deal with a "radical shift in the nature of the wartime battlefield" [33]. This is also reflected when planning, conducting and assessing Cyber Operations. Lacking methodologies that support these actions, significant implications and consequences can be triggered and propagated in unexpected ways: they can impact collateral (military and civilian) actors such as allies, friendly, neutral or even the target or conducting actors. Addressing these issues, this article contributes to the existing body of knowledge from cyber and military domains by proposing an assessment methodology for Military Advantage, Collateral Damage and Military Disadvantage to support military decision makers and their staff when targeting in Cyber Operations.The methodology was validated by military experts on a case study and is the basis for future work on modelling the effects of Cyber Operations.

Acknowledgment

We are grateful to drs. Rudi Gouweleeuw MAJ(R) and prof. dr. Paul Ducheine BG for their valuable feedback and support, and to all participating experts in this research.

References

[1] Ministry of Defence Shrivenham, "Cyber Primer", The Development, Concepts and Doctrine Centre, 2015.
[2] J. Kallberg and B. Thuraisingham, "Cyber operations: Bridging from concepts to cyber superiority", Joint Forces Quarterly, no. 68.1,pp. 53-58, 2013.
[3] C. Maathuis, W. Pieters and J. v. d. Berg, "Cyber Weapons: a Profiling Framework", Cyber Conflict (CyCon US), International Conference on. IEEE, pp.1-8, 2016.
[4] F. Schreier, "On cyberwarfare", Geneva Centre for the Democratic Control of Armed Forces, 2015.
[5] J. L. Samaan, "Cyber command: The rift in US military cyber-strategy", The RUSI Journal, no. 155.6, pp. 16-21, 2010.
[6] J. Goldsmith, "How cyber changes the laws of war", European Journal of International Law, no.24.1, pp. 129-138, 2013.
[7] C. Maathuis, W. Pieters and J. v. d. Berg, "A Computational Ontology for Cyber Operations", ECCWS 2018, 17th European Conference on Cyber Warfare and Security, Academic Conferences and Publishing, 2018.
[8] S. Romanosky and Z. Goldman, "Cyber Collateral Damage", Procedia Computer Science, no. 95, pp. 10-17, 2016.
[9] Council of the European Union, "Avoiding and Minimizing Collateral Damage in EU-led Military Operations Concept", 2016.
[10] NATO, "Collateral Damage Estimation", 2011.
[11] Joint Chief of Staff, "No-Strike and Collateral Damage Estimation Methodology", U.S. Army, 2012.
[12] A. Humphrey, S. See and D. Faulkner, "A Methodology to Assess Lethality and Collateral Damage for Nonfragmenting Precision-Guided Weapons", ITEA Journal, no. 29, pp.411-419, 2008.
[13] S. C. Gordon and D. Douglas, "Modelling and simulation for collateral damage estimation in combat", Enabling Technologies for Simulation Science IX, pp. 309-318, 2005.
[14] M. R. Grimaila, L. W. Fortson and J. L. Sutton, "Design Considerations for a Cyber Incident Mission Impact Assessment", International Conference on Security and Management, 2009.
[15] O. Dogan and K. M. Kosaner, "A Case Study for Cyber Security Assessment on Tactical Command and Control Systems", International Conference on Military and Security Studies, pp. 26-31.
[16] K. Peffers, T. Tuunanen, M. A. Rothenberger and S. Chaterrjee, "A Design Science Research Methodology for Information Systems Research", Journal of Management of Information Systems, no. 24, vol. 3, pp. 45-78, 2008.
[17] J. Iacono, A. Brown and C. Holtman, "Research Methods-a Case Example of Participant Observation", Electronic Journal of Business Research Methods, no. 7, pp. 39-46, 2009.
[18] D. Raymond, G. Conti, T. Cross and R. Fanelli, "A control measure framework to limit collateral damage and propagation of cyber weapons", Cyber Conflict, 5th International Conference on. IEEE, p.1-16, 2013.
[19] D. Gallina, P. Gorman, M. Herman, J. MacDonald and R. Ryer, "Military Advantage in History", Information Assurance Technology Analysis Center, 2002.
[20] NATO, "AJP 3.9 Allied Doctrine for Joint Targeting", 2016.
[21] United States Army Joint Publications 3-12 (R), "Cyberspace Operations", 2013.
[22] United States Army Joint Publications 2-01.1, "Joint Tactics, Techniques, and Procedures for Intelligence Support to Targeting", 2013.
[23] J. Hughes and G. Cybenko, "Three tenets for secure cyber-physical system design and assessment", Cyber Sensing, International Society for Optics and Photonics, vol. 9097, p. 90970A, 2014.
[24] International Committee of the Red Cross,, "Rule 8. Definition of Military Objectives", IHL Database, 1977.
[25] G. McNeal, "The US Practice of Collateral Damage Estimation and Mitigation", Social Science Research Network, 2011.
[26] M. P. Fischerkeller, "Incorporating Cyber Offensive Operations into Conventional and Strategic Deterrence Strategies", Institute for Defense Analyses, 2016.
[27] J. Holsopple, M. Sudit and S. J. Yang, "Impact Assessment", Advances in Information Security no. 62, pp. 219, 2014.
[28] W. S. Powell, Methodology for Cyber Effects Prediction, Black Hat Technical Security Conference, 2010.
[29] International Committee of the Red Cross, "Practice Relating to Rule 14. Proportionality in Attack", IHL Database, 1977.
[30] M. Nusinov, S.J. Yang, J. Holsopple and M. Sudit, "ViSaw: Visualizing threat and impact assessment for enhanced situation awareness", MILCOM 2009, p.1-7.
[31] [31] M. C. Tremblay, A. R. Hevner and D. J. Berndt, "Focus groups for artefact refinement and evaluation in Design Research", Communications of of the Association for Information Systems, no. 26, art. 27, 2010.
[32] L. Tabansky, "Basic concepts in cyber warfare", "Military and Strategic Affairs", no. 3.1, pp. 75-92, 2011.
[33] N. Solce, "The battlefield of cyberspace: the inevitable new military branch-the cyber force", Alb. LJ Sci. & Tech, no. 18, p. 293, 2008.