ETHICAL DIMENSION OF MILITARY INFORMATION OPERATIONS

EUGENIUSZ CIEŚLAK, AUDRONE PETRAUSKAITE

ABSTRACT
The article discusses the issues related to ethics of military information operations. It tries to explore possible challenges posed by military exploitation of the information domain and its relation to professional ethics. Ethical aspects of military information operations are explored through the lens of traditional concepts of the just war theory. The authors try to examine suitability of the just war theory for the study of an ethical dimension of military information operations.

KEY WORDS
Military, information operations, ethics.

DOI: 10.26410/SF_1/19/8

EUGENIUSZ CIEŚLAK
eugeniusz.cieslak@uph.edu.pl
Przyrodniczo-humanistyczny w Siedlcach

AUDRONE PETRAUSKAITE
audrone.petrauskaite@mil.lt
The General Jonas Žemaitis Military Academy of Lithuania, Vilnius, Lithuwania

Introduction

A Western approach to information warfare that limited it to military operations was harshly confronted with Russian "unrestricted" information warfare that stretched into peacetime and involved all instruments of power orchestrated to influence target audiences' minds. At the same time social media gave individual actors power to fight their own information campaigns regardless of the state affiliation. While issues of cyber warfare have been studied in details in recent years, the ethical side of information operations has not enjoyed similar attention. Western militaries will more and more often face adversaries that are not bound by ethical and legal standards imprinted in our democracies. To be effective against such adversaries they might have to operate on the edge of commonly agreed ethical standards of a just war and on the verge of believed opinions about civilian control over armed forces. As information operations entail influencing enemy, as well as neutral and friendly audiences, they pose a challenge for Western militaries related to military professional standards and ethics. What about lies to a civilian part of the society by the military involved in information operations in peace time? What should be the limits of manipulating minds of allied partners and your own society? How to build trust between civilian and military counterparts involved in information operations and what ethical standards should be observed? How to divide responsibilities and accountabilities between civilian and military actors? How to distinguish legitimate combatants from mercenaries, "useful idiots" or human shields? The authors try to ask down-to-earth questions to spark discussion on ethical issues related to information warfare that military is going to face with dramatically increased intensity over coming years. They believe it will be helpful in defining an ethical framework for military conduct in information operations,

providing at least partial guidance how to navigate military activities in the domain of information.

The scope of military information operations

To start the analysis of ethical dimension of information operations we need to understand what the purpose of information operations is. In broad terms information operations seek to influence the behavior of target audiences by changing their ability to make decisions, while simultaneously defending the friendly capability to make proper decisions[1]. The information is used in a similar way to other instruments of national power. Information operations may range from cyber or kinetic attacks against adversary communication nodes and networks to the use of information media to influence attitudes and behaviors of decision-makers and population[2].

All information operations activities occur within the broader context of the information environment. This environment recognizes the critical role that information and information systems play in today's advanced societies as they progressed from an agrarian society to an industrial one, and then to the information age. The information environment pervades and transcends the boundaries of the land, sea, air, space, and cyberspace. What makes information operations different from classical "kinetic" military operations is the fact that it may be accessed and leveraged not only by states but also non-state actors. One may argue that there are no significant differences in access to the information environment between the two types of actors, which makes an "information battlefield" crowded by numerous actors of various affiliations and status.

When discussing information operations we need to be aware of three conceptual dimensions of the information environment: connectivity, content and the cognitive dimension[3]. They all play an important role in information operations. However; there are different ethical implications for each of them. "Connectivity" refers to the physical or electronic links which enable information exchange and operations against them, and do not pose completely new ethical dilemmas. One must take into account "dual-use" connectivity which is employed for both, military and civilian purposes such as electric grid management networks etc. However; when talking about "connectivity" we need also to refer to non-technical relationships between people, such as social media communities etc., which may be exploited for information operations purposes[4].

The "content" of information environment includes the words, images, databases, etc. that contain the information itself, as well as actions and inactions to which meaning is ascribed. This dimension of the information environment links the physical real world with the human consciousness of the cognitive dimension. "Content" of the information environment may constitute for human actions a source of input (stimulus, senses, etc.) and convey the output (intent, direction, decisions, etc.)[5]. There is a significant imbalance between democratic states and their militaries versus non-democratic states along with non-state actors in creating and dissemination

[1] Department of Military Strategy, Planning, and Operations, *Information Operations Primer. Fundamentals of Information Operations AY 2012*, U.S. Army War College, Carlisle, PA, 2011, p. 3

[2] G.R. Lucas, Jr., Just War and Cyber Conflict. "Can tere be an 'Ethical' Cyber War?", lecture at the U.S. Naval Academy, 2014, https://www.usna.edu/Ethics/_files/documents/Just%20War%20and%20Cyber%20War%20GR%20Lucas.pdf (15.03.2019)

[3] Information Operations Primer…, op. cit., pp. 4-5.

[4] European Parliament, Computational propaganda techniques, http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/628284/EPRS_ATA(2018)628284_EN.pdf

[5] Information Operations Primer…, op. cit., p. 4.

of "content" in the information environment. We expect that a democratic state should not use lies – especially against its own society or the international community. A small number of "tactical lies" may turn in the long term into "strategic distrust" that will adversely impact political and social support for specific military operations. On the other hand, non-state actors and undemocratic regimes enjoy relative freedom of lying, at least in the short term. Such a situation creates an ethical dilemma about manipulating information, using lies or not telling the truth to the society.

The "cognitive" dimension of the information environment exists in human minds. In the "cognitive" sphere, the individuals interpret the information, shape opinions and beliefs. In the "cognitive" sphere, the information is filtered and a sense of meaning and context is attached to it. The information is evaluated and processed to form decisions, which are communicated back through the information dimension to the physical world. Although the cognitive dimension cannot be directly attacked it may be influenced indirectly through the physical and information dimensions. Ultimately, the cognitive dimension is the high ground in information operations, the place in which objectives of those operations are achieved. We may view an impact on the "cognitive" dimension using two not fully separated perspectives of the short term and the long term ones. A single piece of fake news creates the short term impact, but what about a prolonged campaign of disinformation? Isn't it a weapon of the mass "consciousness destruction"? What types of attacks against human consciousness should be accepted and which should be banned?

Ethics and military information operations

Ethical problems of information operations may be viewed through the lens of the concepts of the just war theory including *jus ad bellum* and *jus in bello*[6]. Commonly recognized tenets of the just war include a right purpose, duly constituted authority and last resort, while just warfighting takes into account a non-combatant immunity, proportionality and doing more good than harm[7].

The first ethical dilemma related to military information operations stems from blurred lines between the peacetime, crisis and war. In physical domains of the land, sea, air and space, it is quite easy to recognize threats to peace, violations to peace and acts of aggression. It may be difficult to attribute those acts to specific state or non-state actors, but the possibility of plausible denial by an aggressor is becoming slim in recent years. The situation is not as clear with military information operations. The first and most important question that should be asked in the case of information interference is at which point adversary information operations pass the threshold of war. It is of importance as exercising the right of self-defense is commonly viewed as a right reason for a state to go to war. But, how to make sure that a state possesses reliable knowledge that it has fallen victim to an information attack that threatens its territorial integrity, population security or in-

[6] P. Vallely, *The new military morality: Can the principles of Just War have meaning in today's world*?, Independent, 21September 2014, https://www.independent.co.uk/voices/comment/the-new-military-morality-can-the-principles-of-just-war-have-meaning-in-todays-world-9747136.html

[7] W. Yurcik, *Information Warfare: Legal & Ethical Challenges of the Next Global Battleground*, The Proceedings of The Second Annual Ethics and Technology Conference (Ethics'97), Loyola University Chicago, Chicago, IL. USA, June 6-7, 1997, pp. 8-9.

terests?[8] It might be difficult to draw the dividing line between criminal offences in the information environment and those actions of state and non-state actors that constitute acts of war. One must be aware of dynamics of information operations. Military operations conducted in physical domains require time to deploy forces. There is tyranny of physics and geography in the land, sea, air and space operations. Traditionally, military commanders and staffs examine factors of time, space and forces to see the limitations to operations conducted in the land, sea, air and space environments. But the information operations are not so constrained in terms of physical factors. Given an access to a target audience, information operation may escalate within minutes over intercontinental distances, and the volume and content may switch from defensive to offensive even faster via instant messaging. The information influence that may look at the beginning like exercising freedom of discussion by a part of society may turn out to be an integral element of an information campaign by an adversary state to paralyze our ability to react to negative developments in the security environment. Overreacting to freedom of discussion runs against democratic values so it may be difficult to strike a right balance between situational awareness, defensive and offensive information operations.

Military information operations create ethical challenges as it is very difficult to ascertain who is the enemy and what type of protection the non-combatants deserve. The tenet of duly constituted authority has been understood for a long time as waging wars by states, not by individuals. During operations conducted in physical domains every soldier wears a uniform that clearly marks his or her state affiliation. It is what makes them lawful combatants, operating on behalf of a specific state and it is what keeps states accountable for the actions of their soldiers. But that is not the case for information operations. Beside the doubts whether we are at war or not, it may not be certain who we are fighting against. In the information environment non-state actors enjoy almost the same freedom of actions as states. They are able to use commercially available "connectivity" to deliver "content" that influences targeted decision-makers and societies' "consciousness". What state can do to stop non-state actors in the information environment is to cut off "connectivity", for example block IPs, turn down the Internet servers etc. Those options are technically viable but socially unacceptable in Western democracies. Again, defense in the information environment against information operations by non-state actors may demand actions that infringe into your own society and citizen's rights related to free access to information.

Finally, as recent Russian information operations against Western democracies revealed, initiating defensive information operations requires careful consideration of the tenet of last resort. Is it better to ask an adversary to cease his information operations or to start our own ones? One has to understand the inherent risks related to escalation of hostilities and bear in mind that escalation may pass from the information environment into the physical one creating political, economic or even military tensions[9]. For small countries, like Estonia in 2006 or the Baltic States after 2014, subjected to information operations by a powerful neighbor using non-state

[8] P. Kilner P., *Ethics of cyber operations: 5th domain creates challenges, needs new rules,* December 21, 2017, https://www.ausa.org/articles/ethics-cyber-operations-%E2%80%985th-domain%E2%80%99-creates-challenges-needs-new-rules (Accessed 10 March 2019)

[9] J. Arquilla, Ethics and Information Warfare, in: Z. Khalilzad, J. P. White, A. W. Marshall (Ed.), *Strategic Appraisal. The Changing Role of Information in Warfare*, RAND Santa Monica, CA, 1999, pp. 389-391

"green people" to reach consciousness of targeted populations, the situation is even more complicated. Would it be a viable option to initiate defensive information operations or try to pretend that nothing really happened? But trying to pretend that nothing has happened translates into lying to your own society and, at the same time, encouraging further information attacks. Being confronted with such a dilemma might be an uneasy scenario for any government; and for a democratic government this might be especially difficult.

After more than a century of the industrial age, and wars that were fought based on a rather detailed and constantly developing law of armed conflict, we have entered the age of information warfare. Some experts argue that we have been witnessing emergence of the fifth domain of operations. The real difference however, if we compare the information domain to the other four (land, sea, air and space), is that it stretches directly to a cognitive sphere of every single individual exposed to an information activity. Because of that waging military information operations justly (*jus in bello*) may differ from the classical concepts of warfare. The commonly recognized rules of the law of an armed conflict insist that in land, sea or air military operations non-combatants should be protected from military operations and not targeted in a deliberate manner. There is consensus that there should be a clear and visible distinction between combatants and non-combatants. In military land, sea or air operations, civilians carrying and shooting weapons lose their status of non-combatants and become unlawful combatants. But in information operations the situation may be quite different. Non-combatants may be deliberately targeted by adversary's information operations to erode society's support to its own government actions. Beside the short term, tangible results like a decrease of social support for specific actions of the government, one needs to think about the longer term consequences that transgress a "tactical" dimension of information warfare. Targeted communities may develop distrust and cohesion of the society may be threatened. It seems especially easy in multiethnic societies, in which cultures and religions differ. But, it proved also to be possible in ethnically homogenous societies, where dividing lines were drawn along political issues such as democratic rules procedures, social participation in government or historic policy[10]. Societies exposed to a targeted information influence may suffer from "strategic" effects of information operations. The long term decrease in levels of social confidence and willingness to engage in civic activities may be observed. As people injured during classical wars lost their legs or arms, the victims of information operations may suffer from losing empathy and may become paranoid-conspiracy theory-driven believers. At best, they may become reluctant skeptics not willing to engage in civic activities. The ethical challenges related to non-combatants in information operations have also another side. The civilians operating as part of irregular actors or just "lone wolves" become more and more often combatants. Some of them become combatants in a deliberate way because they choose to do so. Some of unaffiliated civilians may be willing to fight information war but they are not aware of all consequences of becoming an unlawful combatant. Finally, there are "useful idiots" that re-tweet the content, like it and share

[10] E. Lucas, P. Pomeranzew, *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda. , Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*, CEPA, August 2016, pp. 30-32

it etc.[11] So there will be an ethical dilemma how to distinguish between them and how to deal with them depending on how guilty they are. The consequences are dire. If a state overreacts and punishes innocent civilians it will act against the core values of democracy. But if a state neglects unlawful combatant actions it may ultimately lose the information fight.

Proportionality is another issue that differentiates information operations from classical, kinetic warfare. In an ideal world we should be able to respond to an adversary information attack in a very precise manner, in a tit-for-tat fashion. We need to calculate possible results of our response, and consider whether some amount of lethal force is needed. But depending on who is the adversary a proportional response may create another dilemma – a risk of escalation. A number of states have already declared their willingness to use lethal force in response to cyberattacks. It might be even more challenging to retaliate against non-state actors in a proportional way. Non-state actors do not typically possess their own infrastructure that might be a suitable target for kinetic retaliation. Non-state actors seem also less vulnerable to information retaliation. Fake news provide a hypothetical adversary with capability to create instant mass effects. That is why the speed of information requires almost an instant response to fake news, which for a democratic state is supposed to be well targeted and proportional. If a state does not want to create delays in defensive information operations, it needs to consider giving military a sort of decentralized execution authority to respond. That may mean the authority to develop and employ a narrative that impacts the adversary, the international public opinion and your own society. The ethical dilemma is what should be the limits of such authority and how to assure civilian control over information operations. Observing the highest standards of civil-military relations by both politicians and military may prove to be a sufficient prerequisite for such scenarios. However, a lack of trust may hamper defensive operations within an information domain and contribute to the adversary's success. In weak democracies politicians or military may use opportunity to manipulate their own society for specific gains. The worst case scenario may be for a democratic state to win an information campaign but turn into a para-democracy controlled by military and security services.

Finally, one who reflects on ethical aspects of military information operations needs to take into account ethical calculations of engaging in such operations. The ethical employment of military forces in information operations should strive to do more good than harm. We have opinions and beliefs rooted in our life-long experience about what is good and what is wrong. It took humans centuries to recognize and accept tenets of the just war and waging wars in a just way. The information environment constitutes, to some extent, uncharted waters. We may think that we know where we are heading with information operations in the short term, but only speculate about consequences of military actions in the information domain further in the future. This will require careful ethical calculation while choosing options for military information operations. It is hard to predict nowadays to what extent it may be desirable to risk actions of the unknown long term consequences, such as the employment of artificial intelligence in an autonomous or semi-autonomous mode to

[11] European Parliament (2018), *Computational propaganda techniques*, http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/628284/EPRS_ATA(2018)628284_EN.pdf

attack human "consciousness"[12]. This scenario however is not a distant future, it is a dilemma for today[13].

Conclusions

Traditional concepts of the just war theory remain valid for physical domains of military operations. But they are not fully applicable to the information environment. Although tenets of *jus ad bellum* and *jus in bello* provide basic guidelines for ethical conduct for the military in information operations, they are not sufficient to address all challenges of the information battleground. Information operations demand more attention to their moral consequences than typical military operations. The boundaries of information operations stretch into cognitive spheres of individuals that are exposed to information influence. As the short-term results of information operations resulting from Russian computational propaganda may be observed in Western societies nowadays, it is hard to speculate about the long-term impact. It is *terra incognita* as our understanding of the information environment and the impact of information on humans is sometimes vague. The long-term impact of deliberate information manipulation on human consciousness is not fully predictable now. The same holds true for social consequences.

Therefore, military information operations are more challenging in ethical terms than those ones that are conducted in traditional domains of the land, sea, air and space. In the worst case scenario information may become a weapon of mass destruction in the "consciousness" domain leaving millions "injured" and distracted for the rest of their lives. In less catastrophic scenarios, it may create conspiracy theories and millions of believers that will not be fully integrated in democratic societies. Ethical calculations of engaging in military information operations should strive to do more good than harm and orient an according categorical imperative. A diligent *primum non noccere* approach should be adopted and "new weapons" in the information environment should be employed in a restrained manner to observe the best tenets of *jus ad bellum* and *jus in bello*.

[12] J.L. Chameau J. L., W. F. Ballhaus W.F., H.S. Lin, (Eds), *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues*, the National Academies Press, Washington D.C. 2014, pp. 51, 55-56.

[13] S. Sanovich, *Computational Propaganda in Russia: The Origins of Digital Misinformation*, Computational Propaganda Research Project. Working Paper No. 2017.3, Oxford University 2017, pp. 15-16

Bibliography

Arkin R.C. (2009), *Ethical robots in warfare*, Georgia Institute of Technology, Mobile Robot Lab, College of Computing, Atlanta, 2009.

Lucas E., Pomeranzew P. (2009), *Winning the Information War: Techniques and Counter-Strategies in Russian Propaganda. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*, CEPA, August 2016.

Arquilla J. (1999), Ethics and Information Warfare, in: Khalilzad Z., White J.P., Marshall A.W. (Ed.), *Strategic Appraisal. The Changing Role of Information in Warfare*, RAND Santa Monica, CA, 1999.

Chameau J.L., Ballhaus W.F., Lin H.S., Editors (Eds) (2014), *Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues*, the National Academies Press, Washington D.C.

Department of Military Strategy, Planning, and Operations (2011) *Information Operations Primer. Fundamentals of Information Operations AY 2012*, U.S. Army War College, Carlisle, PA.

European Parliament, Computational propaganda techniques, http://www.europarl.europa.eu/RegData/etudes/ATAG/2018/628284/EPRS_ATA(2018)628284_EN.pdf

Kilner P. (2017), *Ethics of cyber operations: 5th domain creates challenges, needs new rules*, https://www.ausa.org/articles/ethics-cyber-operations-%E2%80%985th-domain%E2%80%99-creates-challenges-needs-new-rules

Rowe N.C., *The Ethics of Cyberweapons in Warfare*, International Journal of Cyberethics, Vol. 1, No. 1, pp. 20-31, January-March 2010.

Sanovich, S. (2017), Computational Propaganda in Russia: The Origins of Digital Misinformation, Computational Propaganda Research Project. Working Paper No. 2017.3, Oxford University.

Vallely P., *The new military morality: Can the principles of Just War have meaning in today's world*?, Independent, 21 September 2014, https://www.independent.co.uk/voices/comment/the-new-military-morality-can-the-principles-of-just-war-have-meaning-in-todays-world-9747136.html

Woolley S.C., Howard P. N., *Political Communication, Computational Propaganda, and Autonomous Agents. Introduction*, International Journal of Communication 10(2016), 4882-4890.

Yurcik W., (1997), *Information Warfare: Legal & Ethical Challenges of the Next Global Battleground*, The Proceedings of The Second Annual Ethics and Technology Conference (Ethics'97), Loyola University Chicago, Chicago, IL. USA, June 6-7, 1997.http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.15.2345&rep=rep1&type=pdf (accessed 15 March 2019).

EUGENIUSZ CIEŚLAK An university professor at the Institute of Social Sciences and Security Studies, Faculty of Humanities, the University of Natural Sciences and Humanities in Siedlce, Poland. A graduate of the Air Force Academy in Dęblin, Poland and postgraduate studies at the Air University, USA. He holds doctorate and post-doctorate degrees awarded by the Academy of National Defence in Warsaw, Poland in the field of military sciences. His research interests include security and defence policy, military crisis response operations, air operations and air defence.

AUDRONE PETRAUSKAITE An university professor at the Department of Humanities, the Lithuanian Military Academy in Vilnius, Lithuania. A graduate of the Vilnius University, Lithuania. She holds doctorate degree in history awarded by the Sankt Petersburg University, Russia in the field of military sciences. Her research interests include national security, military ethics, civic society and professional military education.