BUILDING THE ETHICAL CYBER COMMANDER AND THE LAW OF ARMED CONFLICT

Jody M. Prescott

Reprinted from
RUTGERS COMPUTER & TECHNOLOGY LAW JOURNAL

BUILDING THE ETHICAL CYBER COMMANDER AND THE LAW OF ARMED CONFLICT

Jody M. Prescott*

I. INTRODUCTION

The importance of ensuring that military action conforms to the overarching political, social, and legal norms held by most democracies[1] means that instruction in military ethics and the law

* Senior Fellow, West Point Center for the Rule of Law; adjunct professor, Department of Political Science, University of Vermont. The opinions expressed in this article are mine alone and not of any U.S. government agency.

1. *See* Jessica Wolfendale, *What is the Point of Teaching Ethics in the Military?*, *in* ETHICS EDUCATION IN THE MILITARY 161, 162 (Paul Robinson et al. eds., 2008) (stating that "[k]nowing the purpose of ethics education and training will determine how and by whom ethics is taught, which ethical theories are taught, and how military personnel should be encouraged to think about military ethics and their roles as members of the Profession of Arms, a profession which must maintain the support and trust of the civilian population if it is to be morally different from mercenary forces.").

of armed conflict (LOAC) is standard fare in military educational and training institutions throughout the world.[2] What are considered "military ethics" appear to vary significantly depending upon the country and the armed service in which they are taught, and in large part appear to focus on the teaching of specific virtues, such as integrity and loyalty, rather than the broad philosophical enquiry found commonly in ethics classes in civilian institutions.[3] There are variations, of course. Military ethics as taught in the Netherlands appear to be consistent with the "Dutch approach" of reducing the amount of force used in operations and emphasizing cooperation, and are therefore geared towards a more critical ethical perspective.[4] Military ethics as taught in Israel favor embedding the ethical lessons in professional development projects linked to officers' sense of professional identity.[5] Given the complementary nature of just war theory and LOAC,[6] it is not surprising that many military academies include some instruction on ethical models on the use of force, but this is far from universal.[7] To further complicate the ethical picture, despite the universal

2. Paul Robinson, *Introduction: Ethics Education in the Military*, *in* ETHICS EDUCATION IN THE MILITARY, *supra* note 1, at 1, 1-5.

3. *Id.* at 6-7.

4. *See* Peter Olsthoorn, *The Ethics Curriculum at the Netherlands Defence Academy, and Some Problems with its Theoretical Underpinnings*, *in* ETHICS EDUCATION IN THE MILITARY, *supra* note 1, at 119, 119-28.

5. Asa Kasher, *Teaching and Training Military Ethics: An Israeli Experience*, *in* ETHICS EDUCATION IN THE MILITARY, *supra* note 1, at 133, 138-41.

6. *See* Michael J. Davidson, *War and the Doubtful Soldier*, 19 NOTRE DAME J. L. ETHICS & PUB. POL'Y 91, 105, 157-59 (2005) (noting derivative nature of LOAC principles based in part on just war concepts, and the importance of legality in modern formulations of just war theory).

7. *See* Jeffrey Wilson, *An Ethics Curriculum for an Evolving Army*, *in* ETHICS EDUCATION IN THE MILITARY, *supra* note 1, at 31, 38. *See also* Jamie Cullens, *What Ought One to Do? Perspectives on Military Ethics Education in the Australian Defence Force*, *in* ETHIC EDUCATION IN THE MILITARY, *supra* note 1, at 79, 84. The Netherlands, for example, provides little in the way of just war theory instruction at its Defence Academy. Olsthoorn, *supra* note 4, at 128. The British Army focuses instead on LOAC rather than "abstract ethical theory" at Sandhurst. Stephen Deakin, *Education in an Ethos at the Royal Military Academy Sandhurst*, *in* ETHICS EDUCATION IN THE MILITARY, *supra* note 1, at 25.

acceptance of the 1949 Geneva Conventions[8] and the large number of countries that have ratified Additional Protocol I,[9] understandings of LOAC can differ in their interpretation and application.[10] This potentially impacts the ways in which young military students process their ethical education and training.

Conceivably, any instructional failure to strongly link military ethics and LOAC together might not have a discernable negative impact upon the ethical and legal conduct of military operations in the geophysical world. The reinforcing effects of civilian control over militaries, military traditions, discipline and regulations, and the continuing influence of ingrained social, religious and moral values will likely provide a sufficient framework within which most soldiers and officers can function ethically and legally in their regular military operations.[11] However, because of the technological and virtual basis of the human-created domain of cyberspace, future cyber operations are potentially very different from their geophysical world analogs.[12] The potential differences are great enough that different approaches may need to be taken by militaries in educating and training personnel eventually destined to become cyber commanders. For these new methods of cyber conflict training and education to be effective in developing ethical

8. *See generally* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 ; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

9. *See generally* Protocol Additional to the Geneva Conventions of Aug. 12, 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3.

10. Jody M. Prescott, *Training in the Law of Armed Conflict – A NATO Perspective*, 7 J. MIL. ETHICS 66, 67, 70-71 (2008).

11. *See* Robinson, *supra* note 2, at 6-9.

12. Kristal L. M. Alfonso, *A Cyber Proving Ground: The Search for Cyber Genius*, 24 AIR & SPACE POWER J. 61, 61-62 (2010) (explaining that cyber operations are so different from those in the geophysical world that non-traditional techniques will be needed to identify and train future cyber military personnel).

cyber commanders, military ethics and LOAC must be integrated. This need for integration is addressed in a lesson plan titled *Ordinary Soldiers*, which was developed by historians, educators, and lawyers under the guidance of the US Holocaust Memorial Museum and the West Point Center for Holocaust and Genocide Studies. This lesson plan not only provides a model for teaching military ethics and LOAC in a complementary manner, its format replicates aspects of how undergraduates interact with their peers in an environment influenced by information technology – an environment which parallels the operational cyber environment of the future in many ways.

This article will first review the current nature of conflict in cyberspace, and then assess current trends in the development of cyber means and methods to form a picture of potential operational characteristics of cyber conflict, including the need for accelerated, but still LOAC-compliant, decision-making by cyber commanders. Next, this article will examine possible ways in which decision-making could be accelerated and surged as necessary, including the use of Autonomous Decision-Making Processes (ADPs) to control and exercise certain uses of force in cyberspace, and the ethical and legal concerns that might flow from the use of these techniques. Mindful of these possible staffing and technological solutions, this article will then address current academic efforts in the areas of cyber operations with respect to military ethics and LOAC, and identify both positive and negative aspects of these efforts. Finally, this article will describe the *Ordinary Soldiers* lesson plan's peer-to-peer (P2P) format as used with U.S. Army cadets at the University of Vermont and Norwich University, as well as its potential to be developed further through the incorporation of social media in its delivery, and propose it as a basis for effectively combining the teaching of military ethics and LOAC for tomorrow's cyber commanders.

II. WILL CYBER CONFLICT BECOME CYBER WAR?

Whether war, commonly understood as armed conflict that results in human casualties and damage and destruction of property and environments, will actually occur as a result of military operations in cyberspace remains an unsettled issue.[13] Although the instances of cyber operations with effects in the geophysical world typically associated with kinetic military actions are at the moment apparently few,[14] the feasibility of causing actual physical harm has been convincingly demonstrated in testing[15] and in the cases of Stuxnet[16] and Shamoon[17] in the field as well. Importantly, these few instances differ markedly from the popular picture of cyber armed conflict often painted by national security officials and others. Rather than occurring at the speed of light and resembling an "electronic Pearl Harbor,"[18] they have instead largely played out quietly and stealthily.[19]

This might change in the foreseeable future, however. A number of NATO nations have publically stated that they possess some "offensive" cyber capacity,[20] and U.S. research and development

13. *See* Thomas Rid, *Think Again: Cyber War*, FOREIGN POL'Y, Mar.-Apr. 2012, at 80-84, *available at* http://www.foreignpolicy.com/articles/2012/02/27/cyberwar (stating that acts of damaging sabotage and terrorism are possible, but war, i.e., an act which is potentially violent, purposeful, and political, is unlikely).

14. *See generally* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012 (Jason Healey ed., 2013) (arguing that actual cyber security concerns are quite acute, but descriptions of "cyber war" are exaggerated).

15. Jeanne Meserve, *Sources: Staged Cyber Attack Reveals Vulnerability in Power Grid*, CNN (Sept. 26, 2007), http://www.cnn.com/2007/US/09/26/power.at.risk/.

16. David Kushner, *The Real Story of Stuxnet*, IEEE SPECTRUM, Feb. 26, 2013, *available at* http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

17. Jason Healey, *Part 1: A Brief History of US Cyber Conflict*, *in* A FIERCE DOMAIN: CONFLICT IN CYBERSPACE, 1986 TO 2012, *supra* note 14, at 14, 76-77.

18. *Id.* at 33.

19. *Id.* at 85.

20. *See, e.g.*, John Leyden, *Germany Reveals Secret Techie Soldier Unit, New Cyber Weapons*, THE REGISTER (June 8, 2012), http://www.theregister.co.uk/

programs suggest a trend towards the industrialization of cyber conflict.[21] This makes it more likely that cyber offensive capabilities will at some point be weaponized in a manner that will make their use more practicable and predictable than the somewhat boutique practice of cyber mischief, which is the norm today.[22] This degree of utility would also suggest that the decision making associated with the use of these capabilities would need to occur more quickly, and would need to be pushed down to lower levels of weapons release authority to take action.[23]

As nations move toward securing the means to conduct cyber conflict[24] that begins to approach our common understandings of war, a consensus appears to be emerging among international organizations concerned with the implementation of LOAC, and in academia, that LOAC at least applies to those actions in cyberspace that either result in, or are intended to result in, injury to humans and damage to geophysical things.[25] In particular, the recently published TALLINN MANUAL marks an important milestone in the understanding of the practical application of LOAC to cyber

---

2012/06/08/germany_cyber_offensive_capability/; Andy Bloxham, *Cyber Weapons Now 'Integral Part of Britain's Amour*,' THE TELEGRAPH (May 31, 2011, 7:13 AM), http://www.telegraph.co.uk/news/newstopics/onthefrontline/8546921/Cyber-weapons-now-integral-part-of-Britains-armoury.html.

21. *See* Special Notice: Plan X Proposers' Day Workshop, DARPA-SN-12-51 (Aug. 17, 2012), *available at* https://www.fbo.gov/index?s=opportunity&mode=form&id=19cced1c188775a844f889872c64c30f&tab=core&_cview=1 [hereinafter Plan X].

22. *See* Rid, *supra* note 13, at 83 (stating that current malicious code can be expensive to acquire, undependable, and likely has a short shelf-life).

23. *See* Zachary Fryer-Biggs, *Slowed by Debate and Uncertainty, New Rules Green Light Response to Cyber Attacks*, DEFENSENEWS (May 27, 2013, 3:45 AM), http://www.defensenews.com/article/20130527/DEFREG02/305270014/ (stating that, while approval of new cyber rules of engagement allow military commanders to respond defensively, "pre-emptive offensive action would still require presidential approval.").

24. Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L R. RED CROSS 533, 534-35 (2012).

25. *Id.* at 545-46. There still appears to be a lack of consensus on whether severe, indirect effects in the geophysical world would be sufficient to find that an armed attack occurred, and therefore also covered by LOAC. *Id.* at 548.

operations. Accordingly, future cyber strike capabilities which produce effects that ripple into the geophysical world, whether used offensively or in self-defense, would require commanders to be responsible under LOAC for their actions and those of their subordinates. Below the level of this use of force, cyber operations that result only in direct effects within cyberspace itself would not be considered uses of force regulated by LOAC, even though their indirect effects might have far-reaching and negative impacts upon the nation targeted.[26] As perhaps best illustrated publicly by the various U.S. cyber strategies and statements of U.S. officials, however, it appears that nations might view this second level of cyber actions in a somewhat amorphous manner.[27] This "grey zone" between the use of kinetic-like force at the upper end, and mere cyber annoyance at the lower, might be further stratified by classified "red-lines" past which nations will not tolerate interference in their national digital infrastructure, and might respond with the use of kinetic-like or even actual kinetic force to unfriendly intrusions.[28]

From a legal perspective, then, a cyber commander might view operations in cyberspace as similar to a game of three-dimensional chess, with different rules at different levels, and the possibility that the effects of play on one level might ripple onto another. At the lowest level, cyber annoyance, domestic law is likely applicable, but it is difficult to conceive of international law concerned with the use of force, armed or otherwise, being applicable. At the highest level, LOAC would operate as *lex specialis* regarding the

26. A minority of the International Group of Experts who compiled the TALLINN MANUAL believed that operations that resulted in these sorts of effects should be considered attacks. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 105-109 (Michael N. Schmitt, ed., Cambridge Univ. Press 2013) [hereinafter TALLINN MANUAL].

27. William J. Lynn III, Deputy Sec'y of Def., Remarks on the Dep't of Def. Cyber Strategy (July 14, 2011), *available at* http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1593.

28. Jody M. Prescott, *Autonomous Decision-Making Processes and the Responsible Cyber Commander*, *in* 5TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 391, 392-93, 407-408 (Karlis Podins et al. eds., 2013).

use of armed force and largely displace other sources of international law,[29] and the rules of engagement (ROE) would be consistent with it. In the grey zone, however, *jus ad bellum* and the ordinary international law regarding the use of non-armed force would apply, as well as other bodies of international law and perhaps even domestic laws to a degree. Cyber ROE at this level would, of course, need to be consistent with controlling law and might even reflect certain ethical concerns under just war theory, but because they would likely be influenced by pragmatic national policies which themselves could be classified, they might be less transparent and therefore less commonly understood than those ROE which implement LOAC in the geophysical world. Making sense of this aspect of operational complexity could challenge the most capable cyber commander even if she had the advantage of operating in an environment that moved no faster than the speed of ordinary human thought – an advantage she would be unlikely to enjoy if in fact cyber operations do become industrialized.

III. ACCELERATING REAL-TIME DECISION-MAKING

To a cyber commander, the rules which she must follow in conducting operations might seem dauntingly complex. Adding to that complexity, she knows that she will be expected to remain effectively in the decision-making loop when the pace of operations might become quicker than she can cogently think. Therefore, not only must she have an accurate visualization of the area of cyber conflict, which might include parts of the geophysical world into which the effects of cyber action might ripple, but she must also be provided with new capabilities to make sound decisions more quickly. These capabilities could include innovative staffing techniques, human computer interfaces (HCIs), and the use of ADPs to execute cyber actions, including the use of armed force.

29. *See* Michael N. Schmitt, *Investigating Violations of International Law in Armed Conflict*, 2 HARV. NAT'L SEC. J. 31, 53-54 (2011).

A. INNOVATIVE STAFFING TECHNIQUES

Innovative staffing techniques could include such measures as organizing cyber command centers so that rather than one weapons release authority or commander, multiple commanders are available to provide a surge capacity of reasoned legal and ethical decision making if the pace or quantum of operations suddenly spiked. Similarly, depending upon targeting considerations such as acceptable levels of collateral damage, commanders could also be organized in a tiered fashion, so that targeting solutions that included the risk of heightened, although still legally acceptable, collateral damage would be executed by higher ranking commanders. For these approaches to work well, however, the commanders would each likely need to be supported by a team of specialist advisors who had long-term training and operational relationships with the commanders and each other, such as cyber technical advisors (TEKADs), political advisors (POLADs), and legal advisors (LEGADs). Developing these specialists, and providing them the education, training, and career opportunities that would make them both well-rounded and tech-savvy, would not likely be cheap.

B. HUMAN COMPUTER INTERFACES

Innovative staffing measures might significantly reduce the time required for cyber commanders to make sound and ethical decisions, but given the pace of possible cyber strike operations, they would not likely be sufficient themselves to ensure such decisions are made in an operationally effective manner. Further, it would be very important to ensure that not only do the commander and her advisor team perceive the same operational picture of the cyber battle space but that the visualization they share is both accurate and readily understandable.[30] Only then would the

30. One of the four key areas to be addressed in DARPA's Plan X is "visualizing and interacting with large-scale cyber battlespaces." Plan X, *supra*

commander be confident that the advice she was receiving was pertinent. For example, research has shown that students using computer interfaces that recognized their individual learning styles showed higher learning results.[31] Through increasing the intimacy of the connections between cyber commanders and their computer systems, tailored HCIs could lessen the amount of time required for a decision to be made by enabling faster exchange of accurate information between commanders, advisor teams, and those computer programs providing situational awareness and analysis.[32] Deep-learning techniques might be used to allow the HCIs to discern the different learning and action styles of different sorts of commanders, and thereby even more finely tailor the representations of the information flow to more closely match the information uptake and action modes of specific commanders.[33]

This tailoring might be even further enhanced through the use of programs that would monitor eye gaze,[34] for example, so that looking at a particular part of a visualization for a sufficient period of time would trigger an additional dash-board style pop-up display that could provide the commander additional information without her having to formally request it.[35] Similarly, a cyber combat dialect using truncated words, phrases, or even gestures could be developed to allow the commander and her advisor team to more quickly orient themselves to the pace of cyber operations in a manner similar to law enforcement officers or pilots using number

---

note 21.

31. Edmond Abrahamian et al., *Is Learning Enhanced by Personality-Aware Computer-Human Interfaces?*, *in* PROCEEDINGS OF I-KNOW '03 228-29 (July 2-4, 2003), *available at* http://i-know.tugraz.at/wp-content/uploads/2008/11/33_is-learning-enhanced.pdf.

32. Thomas K. Adams, *Future Warfare and the Decline of Human Decisionmaking*, 31 PARAMETERS 57, 66 (2001-2002).

33. John Markoff, *Scientists See Promise in Deep-Learning Programs*, N.Y. TIMES, Nov. 23, 2012, http://www.nytimes.com/2012/11/24/science/scientists-see-advances-in-deep-learning-a-part-of-artificial-intelligence.html.

34. Hayrettin Gürkok & Anton Nijholt, *Brain Computer Interfaces for Multimodal Interaction: A Survey and Principles*, 28 INT'L J. HUM.-COMPUTER INTERACTION 292, 297 (2012).

35. *See Id.* at 303-04.

codes and phrases in the geophysical world. Further, programs could be developed to recognize, verbalize, and display information in this dialect for the commander and her advisor team.[36]

Another option to reduce the time required to make a decision might be found in a subset of HCI, brain-computer interfaces (BCIs). BCIs would measure the commanders' brain activity, and execute actions on the basis of what is recognized in the thought patterns, in a manner similar to the recent demonstration of the use of a paralyzed woman's thought patterns to directly control a remotely controlled prosthetic arm.[37] A BCI could perhaps take the form of a sensor helmet worn on the head,[38] or even electrodes in direct connection with the commander's brain.[39] BCIs raise possible medical and ethical issues,[40] however, and might provide too intimate a connection between cyberspace and the commander's brain to be operationally sound – it would effectively cause the commander to become part of the growing "internet of things."[41] Further, if the BCIs were used by the commanders, then perhaps they would also need to be used by the advisor team. Potentially, this could create a discordant muddle of thoughts that would in fact delay the decision cycle rather than accelerate it. Finally, because cyber commanders would be criminally

36. Markoff, *supra* note 33; DEF. SCI. BD., DEP'T OF DEF., TASK FORCE REPORT: THE ROLE OF AUTONOMY IN DOD SYSTEMS 48 (2012), *available at* http://www.acq.osd.mil/dsb/reports/AutonomyReport.pdf.

37. *See* Jennifer L. Collinger et al., *High-Performance Neuroprosthetic Control by an Individual with Tetraplegia*, THE LANCET (Dec. 17, 2012), http://www.sciencedirect.com/science/article/pii/S0140673612618169.

38. *See* Alessandro Pressaco et al., *Neural Decoding of Treadmill Walking from Non-Invasive, Electroencephalographic (EEG) Signals*, 20 J. NEUROPHYSIOLOGY 212 (2012), *available at* http://jn.physiology.org/content/early/2011/07/11/jn.00104.2011.full.pdf+html.

39. Collinger, *supra* note 37.

40. *See* Jens Clausen, *Moving Minds: Ethical Aspects of Neural Motor Prostheses*, 3 BIOTECH. J. 1493, 1496-98 (2008) (stating medical complications, interference with personality and personal identity, and responsibility for malfunctions are among the ethical issues raised by BCIs).

41. Michael J. Covington & Rush Carskadden, *Threat Implications of the Internet of Things*, *in* 5TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (2013).

responsible for LOAC violations on their watch, it would seem neither ethical nor legal for weapons engagement decisions to be registered and executed solely on the basis of thought. Some sort of affirmative command, whether verbal or key-stroke, or perhaps even a combination of these two forms, might be necessary to establish that an intentional order had actually been given.

C. AUTONOMOUS DECISION-MAKING PROCESSES

Although HCIs could further reduce the amount of real time needed for a cyber commander to make a decision whether and how to engage, there will likely still be a quantum difference between this shortened reaction time and the pace at which the cyber operations are actually moving. For a cyber command center to remain operationally effective, there might simply be no other option than to use Autonomous Decision-making Processes (ADPs) to engage with certain weaponized programs. Conceivably, there will likely be few use-of-force issues associated with the use of purely defensive ADPs to maintain the security of a nation's cyber infrastructure. However, once such measures venture beyond the perimeters of their own systems, in what might be called "active cyber defense,"[42] use of force issues under international law do become relevant. Regardless of whether these ADPs are labeled "defensive" or "offensive," if they are either intended to generate effects that cause injury to people or damage to property in the geophysical world, or in fact have that effect, then the issue of command responsibility and potential criminal liability for violations of LOAC arises.

With regard to the use of tangible autonomous weapons systems in the geophysical world, or robotic systems, critics of their use have identified a number of ethical and legal concerns, some of

42. The TALLINN MANUAL defines "active cyber defense" as "[a] proactive measure for detecting or obtaining information as to a cyber intrusion, cyber attack, or impending cyber operation, or for determining the origin of an operation that involves launching a pre-emptive, preventive, or cyber counter-operation against the source." TALLINN MANUAL, *supra* note 26, at 257.

which would be relevant to the use of ADPs in cyber conflict. First, questions have been raised as to whether it is even ethical for computer scientists and engineers to choose to work on military applications at all.[43] Given that the inherent right of self-defense is recognized in the UN Charter,[44] and that many nations have entered into collective security arrangements to defend each other if one is attacked,[45] this likely presents an ethical quandary only for one who is a complete pacifist – and that of course is solved through non-participation. Certain ethicists are also concerned whether the programmers and designers, the manufacturers, or the military personnel who are making use of them could actually be held accountable for LOAC violations resulting from their use.[46] From a practical military legal perspective, these concerns as to whom should be held responsible are of no moment – it is the commander on whose watch these systems are used who is held responsible.[47] The effective and fair implementation of this bright-line test of responsibility, however, potentially comes with both an enormous logistical infrastructure and a lengthy lead time. Before a rational commander would assume her watch in a cyber command center, and affix her digital signature to the electronic log on her computer, she would want to know that the ADPs that would be operational

43. Robert Sparrow, *Building a Better WarBot: Ethical Issues in the Design of Unmanned Systems for Military Applications*, 15 SCI. ENG. ETHICS 169, 170 (2008).

44. U.N. Charter art. 51.

45. *See, e.g.*, North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243 ("The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked . . .").

46. BONNIE DOCHERTY, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS 42-45 (Hum. Rts. Watch ed., 2012), *available at* http://www.hrw.org/sites/default/files/reports/arms1112ForUpload_0_0.pdf.

47. JOINT DOCTRINE NOTE 2/11, THE UK APPROACH TO UNMANNED AIRCRAFT SYSTEMS 5-5 (Ministry of Defence ed., 2011), *available at* http://www.mod.uk/NR/rdonlyres/F9335CB2-73FC-4761-A428-DB7DF4BEC02C/0/20110505JDN_UAS_v2U.pdf [hereinafter UK APPROACH].

during her watch behave as they have been programmed and have consistently predictable effects when they are used in a variety of circumstances,[48] and that they have been created with the necessary ethical and legal oversight and input to ensure their compliance with LOAC and ROE.

Other ethical concerns are not so neatly disposed. One such concern is whether an ADP actually performs as it is programmed, because failure to complete its assigned task properly could result in greater danger to human lives.[49] A second concern of this nature is whether the ADPs are constructed in such a way that there are moral buffers between the execution of their functions and the responsibility of those who are operating them, such that ADP actions are seen by human operators as the result of the ADPs acting according to their design, rather than human operators accepting responsibility for what occurs.[50] A third concern is whether ADPs could possibly be sophisticated enough at this stage of the development of artificial intelligence to discern whether a target that meets objective criteria indicating it is hostile is actually still a threat, or whether it wants to surrender.[51]

Ethical concerns have also been raised as to the potential for psychological stress upon the human operators because they are likely to become emotionally involved in the action even if they are not physically present at its site.[52] Conversely, some have raised concerns that the remoteness of human operators and the possibility that the action might be viewed as a video game might increase the chance that LOAC violations would be committed because the action does not seem real to operators.[53] It has long been recognized that individuals will have different psychological reactions to the same stimuli,[54] so conceivably some cyber

48. *See* Markoff, *supra* note 33.
49. Sparrow, *supra* note 43, at 172-73.
50. *Id.* at 183.
51. *Id.* at 177-78.
52. *Id.* at 174-75, 180.
53. *Id.* at 179, 183.
54. *See, e.g.*, Marilyn Laura Bowman, *Individual Differences to*

operators could care too much about the injury and damage that occurs as a result of using an ADP, while others might distance themselves emotionally from what happens by downplaying its significance. Care must be taken in the design of the HCIs used by the cyber operators to ensure the visualizations they have of the portions of the geophysical world into which the effects of cyber actions might ripple are both accurate and psychologically appropriate.[55] It might also be necessary that counselors are available to assess operators' attitudes and perceptions.[56] These are important concerns worth discussing, and highlight the attention that must paid to the design and function of any ADP's ethical components, discussed in more detail *infra*.

To achieve the level of confidence in the ethical and legal operation of ADPs necessary to assume responsibility for their effects, the commander would need to have been taught how these ADPs were designed and constructed, and to have had the opportunity to work with them on a realistic cyber training range so she knew how they actually performed.[57] Further, to be most effective, her education and training on LOAC, military ethics, and ROE should have occurred in circumstances that replicate, in large part, the information environment she would find herself working in as she conducts cyber operations – "train the way you will fight."[58] This suggests that the instructional methodology should

---

Posttraumatic Distress: Problems with the DSM-IV Model, 44 CAN. J. PSYCHIATRY 21, 25-26 (1999) (explaining that the same traumatic event can cause markedly different psychological responses among victims).

55. Sparrow, *supra* note 43, at 175-76.

56. *See* Anna Mulrine, *Drone Pilots: Why War Is Also Hard for Remote Soldiers*, CHRISTIAN SCIENCE MONITOR (Feb. 28, 2012), http://www.csmonitor.com/USA/Military/2012/0228/Drone-pilots-Why-war-is-also-hard-for-remote-soldiers (stating that U.S. Air Force increases chaplain staffing in UAV units to provide stress counseling).

57. *See* UK APPROACH, *supra* note 47, at 5-5 (explaining that, for the authorizing commander to be fairly held responsible, there would need to be an underlying "assumption that a system will continue to behave in a predictable manner after commands are issued").

58. MARTIN R. STYTZ ET AL., REALISTIC AND AFFORDABLE CYBERWARE OPPONENTS FOR THE INFORMATION WARFARE BATTLESPACE 1-2 (DOD CCRP ed.,

consciously adopt as many of the relevant characteristics of the operational context as possible.

D. ARE ETHICAL AND LEGALLY-COMPLIANT ADPS FEASIBLE?

Before embarking on an expensive and labor-intensive creation of a comprehensive education and training curriculum for future cyber commanders so that they can confidently and effectively use ADPs in a legal and ethical manner when necessary, it is important to first assess whether it is even possible to build ADPs that operate in a predictable, ethical, and legal manner. Recent and important work in the field of robotic weapons programming by Professor Ronald Arkin suggests that programming architecture could be developed so that ADPs both comply with LOAC and meet ethical requirements as to the use of force. As a threshold matter, Arkin's work suggests that this would require the creation and maintenance of an accurate common operational picture of the cyber battle space, the segregation of ethical decision-making authority within the programming, and the appropriate representation of the content of ethical decisions in the programming.[59] Importantly, the nuanced understanding of the operational picture and the judgment upon which a human operator would rely in making a targeting decision are not relevant, as the programming would be designed to err heavily on the side of caution. For example, an autonomous weapon system could not engage a target with lethal force unless there was a certain continuous level of quality in the situational awareness upon which the system relied. Setting this threshold at a level at which there was really no doubt as to whether the possible target was in fact a combatant, would, in Arkin's view, enhance target discrimination, and prevent the engagement of civilians, civilian objects or friendly forces throughout the course of the

2003), *available at* http://www.dodccrp.org/events/8th_ICCRTS/pdf/123.pdf.

59. *See* RONALD C. ARKIN, GOVERNING LETHAL BEHAVIOR IN AUTONOMOUS ROBOTS 69-91 (2009).

engagement.[60] This threshold could be reinforced by complementary measures, such as requiring the weapon system to have consistent information from multiple sensors at all times during the engagement.[61] Dipping below any of these thresholds would prevent the engagement of the target.

As to the segregation of ethical responsibility, Arkin advocates the use of four separate functions to ensure conformance with ethical standards.[62] The first is an "ethical governor," which would conduct an evaluation of the ethical appropriateness of any ADP-proposed lethal response.[63] The ethical governor would be complemented by "ethical behavior controls," which would allow the system to propose only those responses consistent with LOAC and the applicable ROE,[64] and by "ethical adaptors," which would monitor ongoing cyber responses and interrupt the engagement if certain thresholds were exceeded.[65] A geophysical world analog to these functions would be providing legal advice in a targeting cell to a commander as to proposed courses of action as a target is about to be engaged, and the viewing of near real-time video feed of the target site that could provide a sound basis for aborting the attack if the situation changed;[66] for example, if a civilian herding cattle ambled into the attack-effects area prior to a planned strike. Arkin's fourth component is a "responsibility advisor," which is "part of the human-[computer] interaction component" that is used to secure permission from the commander for the ADP to engage in

60. *Id.* at 199-200.

61. *Id.* at 120-21.

62. *Id.* at 126.

63. *Id.* at 127. The governor essentially serves as a cross check on the response proposed by the ADP. *Id.* at 125.

64. *Id.* at 133-34. Further, actions deemed to violate LOAC requirements as programmed would never be undertaken, nor would actions permitted under the ROE but in violation of LOAC. *See id.* at 211.

65. *Id.* at 138-39.

66. *See* UK APPROACH, *supra* note 47, at 5-1 n.2 (stating that UAVs in Afghanistan use the same ROE and targeting guidance as manned aircraft "but they have the persistence to check and re-check, possibly via legal advisers, that they are compliant" with the ROE).

the mission, and to allow for commander overrides of the ADP's decisions if she believed they were in error.[67] As a corollary to this function, Professor Arkin also envisions the possibility of the ADP having the ability to override the incorrect decision of the human commander.[68]

From an engineering perspective, the legal framework for the ADP's operation could essentially be treated the same as other technical and operating requirements at the beginning of the design process, so it could be included in the specification and design of the various subsystems, as well as informing the concept of employment.[69] It is at this point where fulfilling Arkin's third requirement for the creation of a LOAC- and ROE- compliant ADP becomes potentially problematic. Professor Arkin relies on a combination of philosophical models of conflict ethics such as just war theory and LOAC to provide the content he considers necessary to ensure that the ADPs operate in an ethical manner.[70] Although the just war theory and other ethical thought regarding conflict might very well inform the decision making of the political leaders who approve the ROE, and might have been part of commanders' military ethics education, these models are not used explicitly by commanders in the field in determining when to engage and with how much force. These officers are trained in and conduct exercises in conformance with LOAC, and their operational decisions are regulated by LOAC and LOAC-consistent ROE, not philosophy. The legal and political advice they would receive from their advisors would be cast in this decision-making context.

It is entirely possible, however, that commanders might find themselves operating under ROE that restrict the scope of their

67. ARKIN, *supra* note 59, at 143-53.

68. Tom Simonite, *'Robot Arms Race' Underway, Expert Warns*, NEWSCIENTIST (Feb. 27, 2008, 12:10 AM), http://www.newscientist.com/article/dn13382-robot-arms-race-underway-expert-warns.html.

69. UK APPROACH, *supra* note 47, at 5-2.

70. ARKIN, *supra* note 59, at 37-48, 69-91, 149.

authority to use force in certain situations, under conditions that might appear to reflect certain principles found in different just war theories. For example, NATO air forces in the 2011 campaign in Libya were apparently operating under ROE that caused strikes to be aborted if there was even one known civilian who was put at risk of incidental injury.[71] This rule's consistency with philosophical notions as to the absolute protection of civilians in combat operations under the new just war model of responsibility to protect[72] was likely coincidental. It appears to have been based on the legal scope of the mission as defined by UN authorization, and the realistic political assessment that there would be little domestic support for the mission within many NATO member nations unless there were strict controls put in place to mitigate legal – but operationally counter-productive – collateral damage, rather than on explicit ethical theory.[73]

Additionally, although Professor Arkin sees an important role for ethical advisers and LEGADs as part of the software development team that designs an ADP,[74] it is not certain that governments would actually be willing to include ethical advisers on design teams that are likely required by contract to generate a product in accordance with specifications within a certain period of time, or if they were included, how meaningful a role they would be allowed to play. Further, even if the focus of the program is on legal compliance rather than broader ethical behavior, determining what

71. *Statement by the NATO Spokesperson on Human Rights Watch Report*, NATO (May 14, 2012), http://www.nato.int/cps/en/natolive/news_87171.htm; *See also Canadian Pilots Abort Bombing Over Risk to Civilians*, CTV NEWS (Mar. 22, 2011, 7:55 PM), http://www.ctvnews.ca/canadian-pilots-abort-bombing-over-risk-to-civilians-1.621929.

72. *See, e.g.*, Eric Patterson, *Just War in the 21st Century: Reconceptualizing Just War Theory after September 11*, 42 INT'L POL. 116, 125 (2005), *available at* http://www.u3asunshine.org.au/sc/wp-content/uploads/2012/08/sep11.pdf.

73. *See, e.g.*, David Brunnstrom, *Dutch Warn of Heated NATO Debate as Libya Drags On*, REUTERS, June 29, 2011, *available at* http://www.reuters.com/article/2011/06/29/us-libya-nato-dutch-idUSTRE75S3FW20110629 (describing deep divisions in the Alliance as the scope of the mission evolved).

74. See ARKIN, *supra* note 59, at 95-113.

the legal content of the ADP would be, and how it would be expressed and described, is potentially problematic. For those without practical military experience, such as that gained while working in a multinational headquarters in a theatre of operations, the near universal acceptance of basic LOAC conventions and the significant recognition of important LOAC principles as a matter of customary international law[75] might obscure the degree to which different interpretations and applications of LOAC exist among the military forces of the international community. Moreover, LEGADs are not fungible. In addition to national differences in LOAC training and interpretation and the expression of LOAC advice to commanders, there are experiential differences as well. A LEGAD who has had experience in a combined air operations center or a dynamic targeting cell is likely to provide a design team with a much richer understanding of the significance of the content and context of decisions under LOAC to engage with armed force than is a LEGAD whose knowledge of LOAC is primarily academic.

Additionally, it is not clear that governments would be willing to spend significant sums of money programming ADPs to engage only on the highest level of certainty that a target is proper under LOAC.[76] Engagement on the basis of reasonable certainty is permissible under LOAC,[77] and in certain situations, commanders might believe that it was necessary to increase the level of risk within legal bounds in order to be able to prosecute cyber actions

75. *See generally*, JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (Cambridge Univ. Press 2005).

76. As Professor Arkin describes, his paradigm is consistent with the principle of "first, do no harm," and therefore the ADP "should act conservatively in the presence of uncertainty (doubt)." RONALD C. ARKIN, GOVERNING LETHAL BEHAVIOR: EMBEDDING ETHICS IN A HYBRID DELIBERATIVE/REACTIVE ROBOT ARCHITECTURE, PART III, REPRESENTATIONAL AND ARCHITECTURAL CONSIDERATIONS 121-22 (2008), *available at* https://smartech.gatech.edu/handle/1853/22715.

77. Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation under International Humanitarian Law*, 90 INT'L REV. RED CROSS 991, 1033 (2009).

effectively. This "dialability,"[78] or dynamic scaling of the acceptable risk level in response to situational requirements, although quite legal, might work to undermine Professor Arkin's paradigm of ADP decision making, and it would likely complicate the development of action thresholds within the programming. As Arkin has noted, however, if a commander makes the affirmative decision to accept higher risk of LOAC violation, the decision to change the ADP's setting would need to have been anticipated by the design team so that this acceptance of responsibility by this particular commander could be properly recorded.[79]

This standard of reasonable certainty also provides an answer to the ethical concern raised as to whether the ADP could be sophisticated enough to properly assess if the target wished to surrender. A human combatant is unlikely to know whether an adversary actually has the intent to surrender unless this intent is manifested by specific objective actions on the part of the adversary, such as throwing down weapons, raising arms, and saying, "I surrender." There is no requirement in LOAC that adversaries be given notice prior to engagement that their surrender is requested or that they should be captured instead, contrary to the positions of certain writers,[80] and therefore their specific intent minus any objective manifestations of surrender is not relevant to the issue of whether they may be properly engaged. The content incorporated into the design of the ADP would need to specify the objective manifestations of surrender that would cause the ADP to not engage even if a target otherwise met the criteria for being an enemy combatant. In sum, with Professor Arkin's ADP architecture

78. *Cf.* MARNITA THOMPSON EADDIE, DIALABLE CRYPTOGRAPHY FOR WIRELESS NETWORKS 2-7 (Air Force Inst. Tech. ed., 2008), *available at* http://www.dtic.mil/dtic/tr/fulltext/u2/a487430.pdf (describing dynamic selection of optimal cryptographic algorithms and cryptographic strengths according to available hardware and bandwidth).

79. Sofia Karlsson, *Ethical Machines in War: An Interview with Ronald Arkin*, OWNI.EU (Apr. 25, 2011), http://owni.eu/2011/04/25/ethical-machines-in-war-an-interview-with-ronald-arkin/.

80. *See, e.g.*, Ryan Goodman, *The Power to Kill or Capture Enemy Combatants*, 24 EUR. J. INT'L L. 819 (2013).

there theoretically would be no grey area in which the weapon system would need to try to emulate the complexity of human judgment and emotion in deciding whether to engage – either the target is identified as a combatant with an exceedingly high level of certainty and therefore engaged, or no engagement occurs.[81] Regardless, the standard of reasonable certainty for targeting likely means that even an ethically imperfect ADP would still be good enough to use in combat so long as its ROE were in conformance with LOAC.

IV. CURRENT CYBER EDUCATION EFFORTS IN ETHICS AND LOAC

U.S. military educational and training institutions appear to increasingly focus upon developing cyber talents among cadets and among officers at various levels of their respective careers. The U.S. military academies have established on-campus cyber centers to further promote the study and application of cyber operations.[82] The effort to train new cyber officers is occurring outside the service academy context as well. For example, the U.S. Air Force Institute of Technology's Center for Cyberspace Research conducts a summer program for Reserve Officer Training Corps (ROTC) cadets who are majoring in computer science, computer engineering, and electrical engineering.[83] Similarly, important military educational institutions such as the U.S. Navy's Naval

81. Arkin, *supra* note 76, at 124.

82. *See, e.g.*, Amber Corrin, *Service Academies Ramp Up Cyber Training*, FED. COMPUTER WKLY. (Apr. 26, 2013), http://fcw.com/articles/2013/04/26/cyber-training-academy.aspx; Eric Beidel, *Military Academies Look to Fill Nation's Cybersecurity Gaps*, NAT'L DEF. MAG. (Jan. 2012), http://www.nationaldefensemagazine.org/archive/2012/January/Pages/MilitaryAcademiesLooktoFillNation%E2%80%99sCybersecurityGaps.aspx; *Welcome to the Cyber Research Center*, U.S. MILITARY ACADEMY, http://www.westpoint.edu/crc/SitePages/Home.aspx (last visited Nov. 29, 2013) (detailing West Point's cyber center).

83. *Advanced Cyber Education*, AIR FORCE INST. TECH., http://www.afit.edu/ccr/ace/ (last visited Nov. 29, 2013).

Postgraduate School (NPS) also offer an advanced course of study in cyber operations.[84]

Although it is not clear whether U.S. military educational and training institutions at the undergraduate level have incorporated ethical concerns with regard to the use of cyberspace into their respective military ethics curricula, the need for legal instruction in this regard has been recognized. At the undergraduate level, the U.S. Air Force Academy offers a cyber law course,[85] and the U.S. Naval Academy's Center for Cyber Security Studies now even has a law professor with significant operational cyber law experience as part of its staff.[86] Moreover, the U.S. is not alone in seeking to have this specialization embedded in its educational and training programs, as demonstrated by the Netherlands.[87] As to education of more senior officers, for example, a new course has been created at NPS by Dr. Dorothy Denning, a highly-respected cyber expert and scholar, entitled "Conflict in Cyber Space," that addresses both just war principles and LOAC.[88] This is a required course for the students enrolled in the Cyber Systems and Operations masters' degree program.[89]

Unfortunately, there are few assessments of efforts to include ethics and legal topics in operational cyber instruction available for review in the public domain. One such assessment concerns the U.S. Air Force Academy's Basic Cyber Training Program in the summer of 2011, and this assessment particularly highlights the

84. *Cyber Academic Group*, NPS, http://www.nps.edu/academics/generalcatalog/2529.htm (last visited Nov. 29, 2013) [hereinafter *Cyber Academic Group*].

85. *Law 440*, U.S. AIR FORCE ACAD., http://www.usafa.edu/df/dfl/courses.cfm#Law440 (last visited Nov. 29, 2013).

86. *Robert Clark*, USNA CTR. OF CYBER SEC. STUD., http://www.usna.edu/Cyber/leadership/Clarkbio.php (last visited Nov. 29, 2012).

87. Terry D. Gill & Paul A. L. Ducheine, *Anticipatory Self-Defense in the Cyber Context*, 89 INT'L L. STUD. 438, 444 n. 9 (2013).

88. Kenneth Stewart, *Cyber Security Hall of Famer Discusses Ethics of Cyber Warfare*, NAVY (June 4, 2013, 9:09 PM), http://www.navy.mil/submit/display.asp?story_id=74613.

89. *Cyber Academic Group*, *supra* note 84.

importance of understanding the intersecting issues of personnel selection and educational technique in the delivery of cyber ethics and law training. The Basic Cyber Training Program was developed as a sixty-hour course specifically to give cadets "an understanding of the challenges they might face as officers charged with operating in cyberspace."[90] Appropriately, it was designed primarily as a hands-on, practical training course to introduce cadets who had been chosen as cyber officers to both defensive and offensive cyber operations; it also included instruction on LOAC.[91] The educational demographics of the cadets were very interesting, and are worthwhile of examination in detail.

Many of those assigned to be cyber officers had not chosen the field, and the non-volunteers tended to be below average in terms of academic achievement.[92] Despite these challenges, the overwhelming majority of cadets were quickly able to demonstrate technical proficiency with cyber attacks,[93] perhaps surprising the course authors. As to cyber law, however, the cadets rated this block of instruction the lowest in the course.[94] This too appears to have surprised the course authors, because "many of [the] faculty members who [had] experience in cyber operations found this material fascinating."[95] Unlike the bulk of the course, however, the LOAC lesson was apparently delivered as an interactive discussion rather than being included in the hands-on training with a particular tool.[96] Further, the content of the interactive discussion between the faculty and the cadets appears to have been quite dated. Not only is it not clear whether ethicists or lawyers were involved in this discussion, the material supporting the discussion appears to have

90. David Bibighaus et al., *Effectively Teaching Cyber Warfare to a Non-Technical Audience*, *in* PROCEEDINGS OF THE 7TH INTERNATIONAL CONFERENCE ON INFORMATION WARFARE AND SECURITY 36 (Dr. Volodymyr Lysenko, Ctr. for Info. Assurance and Cybersecurity, ed., 2012).

91. *Id.* at 37.

92. *See id.* at 36.

93. *Id.* at 41.

94. *Id.* at 40.

95. *Id.*

96. *Id.* at 37-38.

been based on Professor Michael Schmitt's early theoretical work in reconciling cyber operations with LOAC from the late 1990s.[97] This is seminal work, but as best shown in the recent TALLINN MANUAL, the writing and editing of which depended heavily upon Professor Schmitt's expertise, thinking on the application of LOAC to cyber operations has advanced tremendously in the intervening decade.[98] In the end, the course authors recommended significantly reducing the LOAC lesson for the next iteration of the course.[99]

Although this one assessment is a very limited basis upon which to base conclusions as to the best way to incorporate ethics and legal topics into a course of instruction, it does suggest certain points worthy of consideration with regard to beginning to build the ethical cyber commander from the ground up. First, simply having the ethics and legal instruction occur at the same time as the technical and operational instruction is probably not sufficient. It must be integrated with the technical and operational instruction in its manner of delivery as well. Second, it should probably be grounded in a factual context to which the cadets could relate and which is easily visualized. Although the technical and operational instruction is likely to be abstract to a degree, its integration with immediate opportunities to apply it to a cyber scenario apparently suffices to make the experience real and interesting for cyber students. Third, the ethics and legal instruction should probably leverage the preferred style in which the young students ordinarily relate to their social and informational environments, i.e., viewed through a cyber-enhanced lens. Students discussing an abstract topic with an instructor, or even a panel of instructors, probably means that only one person is speaking at a time in an ordinary class setting. As facilitated by social media, young students are accustomed to a flattened discussion hierarchy and an accelerated

97. *Id.* at 38 (explaining that it was apparently based on Professor Schmitt's seminal work on cyber military operations and LOAC); *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. TRANSNAT'L L. 885 (1999).

98. *See generally* TALLINN MANUAL, *supra* note 26.

99. Bibighaus, *supra* note 90, at 42.

pace of information exchange – even an "interactive" discussion is probably too slow and too channeled to hold their interest for long.

V. RETHINKING ETHICAL EDUCATION AND TRAINING

As highlighted by U.S. Air Force academy Cyber Basic Course example, and the discussions above regarding the design of ADPs, the differences between the conduct of offensive operations in cyberspace and the geophysical world, and the unique complexities and investment requirements identified in the future use of HCIs and ADPs, likely mean new educational and training techniques must be developed to effectively mold young cyber officers,[100] and tactical and ethical decision-making skills will need to be learned in a complementary and interrelated way. Further, unlike traditional instruction methods, which often tend to be instructor-oriented even if they are interactive discussions, education and training for young cyber officers should not be merely enhanced through the use of cyber technology and social media, but it should also reflect important characteristics of cyber interaction, such as a flattened organizational hierarchy, immediate access to multidisciplinary information, high levels of communication between students during the lessons,[101] and the ability to learn and act as a group to solve complex problems, i.e., a swarm.[102] Recent field testing of the

100. *See* DARYL L. CAUDLE, DECISION-MAKING UNCERTAINTY AND THE USE OF FORCE IN CYBERSPACE: A PHENOMENOLOGICAL STUDY OF MILITARY OFFICERS 259, 280 (Univ. Phoenix ed., 2010), *available at* www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA534888 (explaining that new doctrine and training are required to optimize cyber commander performance).

101. Rachel Happe, *Networks, not Hierarchies: How Social Media is Transforming Office Politics and Changing What We Value in Others*, LABOURLIST BETA (Mar. 8, 2010, 7:03 PM), http://labourlist.org/2010/03/networks-not-hierarchies-how-social-media-is-transforming-office-politics-and-changing-what-we-value-in-others/.

102. *See* Sergio Gutiérrez & Abelard Pardo, *Swarm-Based Techniques in E-Learning: Methodologies and Experiences*, *in* ADVANCES IN E-LEARNING: EXPERIENCES AND METHODOLOGIES 199, 200 (2008).

Ordinary Soldiers lesson plan perhaps provides a starting point for considering how to best deliver this kind of instruction.

A. ORDINARY SOLDIERS – THE CASE STUDY

Premised on MARCHING INTO DARKNESS, Professor Waitman Beorn's recent book on the involvement of regular German armed forces in the Holocaust in occupied Belarus,[103] the *Ordinary Soldiers* lesson plan has enjoyed the ever-increasing use of its modular leadership and ethics case study lesson plan. The case study is based on the actions of the 1st Battalion, 691st Regiment, a rear area security infantry unit, in October 1941, in occupied Belarus. If in fact cyberspace is so different that the ethical and legal education and training of future cyber commanders must be significantly changed for it to be effective, why is a case study of a foreign small unit in an operational backwater over seventy years ago even relevant to modern ethics and leadership concerns? As will be discussed below, the rather ordinary circumstances of this battalion, the clarity of the decision-making by its company-grade officers as to how they dealt with an illegal order to execute civilians, and the rich trial record of individual soldiers' and commanders' recollections and attitudes provides unmatched content for a method of instructional delivery that levers the technology and information environment experienced by today's students. Importantly, given the significant variation between different military educational and training institutions as to the way in which they teach military ethics, the lesson plan is not tied to one particular military ethics model, although the materials for instructors included in the lesson plan provide suggestions for linking the lesson plan with military ethics.

Originally formed as part of a static fortress defense division, the 1st Battalion's first tour of duty in early World War II appears to have been uneventful, as a part of the German force occupying

103. *See* WAITMAN WADE BEORN, MARCHING INTO DARKNESS: THE WEHRMACHT AND THE HOLOCAUST IN BELARUS (2013).

France in 1940.[104] By the late summer of 1941, however, it had already transferred to the Eastern Front and it assumed rear area security duties in Belarus, some 150 kilometers behind the German units advancing on Moscow.[105] Although German forces were concerned about partisan activity in this communications zone, and there were certainly bypassed Soviet units that had not surrendered yet, this rear area appears to have been fairly quiet in terms of military activity once the German front-line units had swept east.[106] Reflecting in large part the demographics of its parent division, 1st Battalion was not a front-line unit. Its members tended to be significantly older than the average German front-line soldier at this early point in the war, and in fact one of its company commanders, First Lieutenant Sibille, was a forty-seven year old school teacher and World War I veteran.[107]

In late September 1941, battalion representatives attended a three day training session held at their Army Group headquarters in Mogilev, Belarus. Here, they received presentations from high ranking SS officers and observed "anti-partisan" operations at the small-unit level that apprehended no partisans but did result in the executions of numerous Jewish civilians.[108] The implicit message of the conference as understood by the German personnel who attended was that Jews were complicit in partisan action, and were

104. XIII, JUSTIZ UND NS-VERBRECHEN, SAMMLUNG DEUTSCHER STRAFURTEILE WEGEN NATIONALSOZIALISTISCHER TÖTUNGSVERBRECHEN, 1945-1966 618-19 (Irene Sagel-Grande et al. eds., 1975) [hereinafter "XIII, JUSTIZ UND NS-VERBRECHEN"]. Composed of older soldiers equipped primarily with weapons captured from the Allies, the Darmstadt State Court noted that the unit was not considered suitable for front line service in the East. *Id.* at 619.

105. EINLAGEATLAS DER OPERATIONSABTEILUNG DES GENERALSTABS DES HEERES [Atlas of Operations Section of the German Army General Staff on the Eastern Front] 85 (2001).

106. Waitman Wade Beorn, *A Calculus of Complicity: The Wehrmacht, the Anti-Partisan War, and the Final Solution in White Russia, 1941-42*, 44 CENT. EUR. HIST., 308, 317-18 (2011).

107. Letter from Christiane Sibille to Dr. Waitman Beorn (Oct. 3, 2010) (on file with Dr. Beorn).

108. Beorn, *supra* note 106, at 319-22.

therefore appropriate targets of anti-partisan operations.[109] Shortly afterwards, in early October, the 1st battalion commander ordered each of his three maneuver infantry companies to kill all the Jews in their respective areas of operation. One company commander complied with the order immediately.[110] The second, First Lieutenant Sibille, refused, and stoutly maintained his disobedience despite being directly ordered again to kill the Jewish civilians.[111] A third declined to carry out the order at first, but upon having the order reaffirmed by the battalion commander, absented himself from the scene of the executions and directed the company first sergeant (the senior non-commissioned officer in the company) to conduct the executions.[112]

Three company commanders in the same unbloodied battalion, each facing almost identical operational circumstances, had three very different responses to the same illegal order. Other than fellow officers apparently considering him weak, nothing happened to First Lieutenant Sibille – he was not punished for his disobedience to direct orders.[113] Interestingly, Sibille was not alone. Research into eighty-five identified instances of German military personnel refusing orders to kill civilians and prisoners of war shows that with the exception of one very specific case, no one who said "no" was prosecuted.[114] Even the one officer who was tried and

109. XII, JUSTIZ UND NS-VERBRECHEN, SAMMLUNG DEUTSCHER STRAFURTEILE WEGEN NATIONALSOZIALISTCHER TÖTUNGSVERBRECHEN, 1945-1966 374 (Adelheid L. Rüter-Ehlermann et al. eds., 1974) [hereinafter XII, JUSTIZ UND NS-VERBRECHEN]. As the U.S. Military Tribunal found in the *High Command Case*, "[w]e have a strong suspicion from the record in this case that anti-partisan warfare was used by the German Reich as a pretext for the extermination of many thousands of innocent persons." *The German High Command Trial, U.S. Military Tribunal, Nuremberg, Dec. 30, 1947 – Oct. 28, 1948*, XII LAW REPORTS OF TRIALS OF WAR CRIMINALS 85 (U.N. War Crimes Comm. ed. 1949) [hereinafter *High Command Case*].

110. XII, JUSTIZ UND NS-VERBRECHEN, *supra* note 109, at 377.

111. *Id.*

112. *Id.* at 375-76.

113. Sibille letter, *supra* note 107.

114. David H. Kitterman, *"No!": Germans Who Refused to Execute Civilians during World War II*, 11 GERMAN STUD. REV., 241, 251 (1988). There is anecdotal

convicted never had his sentence affirmed, and his prosecution appears to have been the result of the very public way in which he not only said "no," but also advised his men that the kill order was illegal and immoral.[115]

B. ORDINARY SOLDIERS – THE P2P LESSON PLAN

After the war, as the Allied occupation of Germany wound down, the third company commander and his first sergeant were tried for murder in domestic German courts.[116] The lengthy trial developed a detailed evidentiary record not just of how the executions were conducted, but also of the impressions of many soldiers and officers of the command climate in the battalion, the leadership qualities of different officers, and the effects of the executions upon the attitudes and emotions of the soldiers who had conducted them. Set against the backdrop of the recently concluded trials of Nazi war criminals before international and U.S. military tribunals at Nuremberg, this record and the courts' findings make the execution order an ideal case study for exploring the relationships between leadership qualities, ethics, and LOAC. The *Ordinary Soldiers* lesson plan synopsizes the historical and evidentiary record, the legal standards that resulted from the Nuremberg trials,[117] and the relationship between LOAC and ROE. It also provides a number of appendices, including a legal perspective on Germany's historical treatment of civilians and partisans both in academic institutions and in the field, a translation of the German appeals court decision in the case, translations of

---

evidence of a German soldier in the Netherlands refusing to serve in a firing squad to execute hostages then being executed with the civilians. JAMES H. TONER, TRUE FAITH AND ALLEGIANCE: THE BURDEN OF MILITARY ETHICS 63 (Univ. Press of Ky. 1995).

115. Kitterman, *supra* note 114, at 246.

116. XIII, JUSTIZ UND NS-VERBRECHEN, *supra* note 104, at 617-44; XII, JUSTIZ UND NS-VERBRECHEN, *supra* note 109, at 371-85.

117. *High Command Case*, *supra* note 109, at 72 (explaining that obedience to illegal orders is not generally a defense); *see id.* at 86 (showing command responsibility for LOAC violations).

different German high command orders applicable to the harsh treatment of civilians and prisoners of war in World War II, and the restricted jurisdiction of courts-martial over German soldiers suspected of criminal acts against these protected persons.[118]

At the U.S. Air Force Academy and the U.S. Military Academy at West Point, and in U.S. Army ROTC programs at civilian universities and Norwich University (a private military academy in Vermont), cadets have received different modules of the lesson plan, ranging from the basic one-hour case study history version to the most intensive version, the six-hour mass small group discussion format. At first blush, "mass small group discussion" sounds oxymoronic. As demonstrated in the proof of concept field test of the module in the spring of 2013 at Norwich University, however, it is a particularly effective means to deliver Peer-to-Peer (P2P) training[119] and, as such, is well-suited for use with university audiences accustomed to the ubiquity and access of today's electronic communications and technology-enabled learning environments.[120]

The six-hour module places the students in the position of U.S. officers who have been appointed by their commanders to conduct an investigation into the circumstances of the execution order given by the 1st Battalion commander. They then report back their findings to the entire class on the causes for the different reactions by the company commanders to the illegal order, assessments of

118. *High Command Case*, *supra* note 109, at 29-31 (translating the Decree on Exercising Military Jurisdiction in the Area of Barbarossa and Special Measures by the Troops, German High Command, May 13, 1941). Most courts-martial for German soldiers committing punishable offenses against civilians in the East were to be suspended. *Id.*

119. The benefits of peer-to-peer education and training in complex topic areas have been recognized in academia. Katharine Mangan, *Teaching Tough Course Led Chemistry Professor to Push Peer Learning Approach*, THE CHRON. OF HIGHER EDUC. (Apr. 24, 2011), http://chronicle.com/article/Teaching-Tough-Course-Led/127240/.

120. ZAHED SIDDIQUE ET AL., ENHANCING PEER-LEARNING USING SMART DEVICES 3-8 (Am. Soc'y for Eng'g Educ. ed., 2013), *available at* www.asee.org/public/conferences/20/papers/6142/download.

potentially moral and legal culpability, and recommendations as to how such atrocities could be prevented in the future. As demonstrated by the successful delivery of the module at Norwich University, intensive preparation allows the cadets to be able to do this effectively within the time constraints imposed by a busy academic and training schedule.

First, freshman and senior University of Vermont (UVM) cadets received the one-hour historical lecture module together. The next week, the senior UVM cadets received instruction on facilitating small group discussions on leadership and ethics using the *Ordinary Soldiers* lesson plan as the basis for the command-directed investigation. In the third week, the senior cadets were then each paired with a group of several freshman cadets, and given two hours to develop a draft investigation report and to report it back to the rest of the class, addressing only those points that had not already been raised by earlier briefers. This accustomed the UVM cadets to working with small groups on the lesson plan, and further normalized the important points that the small groups would need to address to successfully navigate the content of the lesson plan.

In the meantime, at their campus seventy-five kilometers away, over eighty senior Norwich cadets received the historical lecture. One week later, after the UVM small group facilitators had completed their training, the cadets from the two schools met on the floor of the Norwich hockey arena to conduct the mass small group discussion. The UVM small group facilitators each joined a table of six or seven Norwich cadets, and they all spent the first hour in discussion with each other on the topics required to be reported back to the entire group, with faculty members circulating and answering questions as needed. In the second hour, the Norwich cadets who had served as scribes for their respective tables presented to the entire group their discussion results, which were transcribed and projected on a large screen at the center of the table array. Two Norwich cadets majoring in journalism had served as process observers during the discussions, and they then briefed the group on their observations regarding the content of the

discussions, and how they related to the larger topic of finding ways to increase protection of civilians in conflict zones. At the conclusion of the lesson, two Norwich cadets, one man and one woman, were asked to summarize for the group what they believed the important points of the discussion had been regarding the protection of civilians and showing leadership in this regard as new U.S. Army lieutenants.

The cadets' reception of the *Ordinary Soldiers* P2P module was very favorable. The mass small group format allowed highly decentralized discussion of the leadership and ethical issues raised in the case study, and gave cadets who might not have spoken up in traditional instructor-led learning formats an opportunity to register their opinions. The UVM small group facilitators were outsiders to the Norwich cadets in certain respects, but through facilitating small group discussion when it lagged or started to veer off-topic or schedule, rather than leading it, they reinforced each table's flattened discussion hierarchy.[121] These features of the P2P module mimic, in an analog fashion, the nature of modern electronic communication via social media. In the second hour, the reporting of each table's results was done by exception, saving time, and displayed on a large central screen, increasing content uptake among the cadets. The use of a moderator to comment on the results as they were briefed, and to ask the cadets clarifying questions at the same time, streamlined the transmission of information to the entire group. In effect, the lesson plan resulted in a type of swarming by complex agents relying on group intelligence to achieve the optimal solution.[122] Perhaps most

121. *See* THOMAS. L. FRIEDMAN, THE WORLD IS FLAT: A BRIEF HISTORY OF THE TWENTY-FIRST CENTURY 43-45 (Farrar, Straus and Giroux 2005) (detailing how modern electronic devices make it economically feasible for an individual to establish a news website capable of distributing information online and receiving feedback well within the news cycles of established networks); David Boud, *Introduction* to PEER LEARNING IN HIGHER EDUCATION 3-5 (D. Boud et al. eds., 2001) (explaining that the essential characteristic of P2P learning, regardless of its specific format, is that the participants exercise no power over each other as a function of position or responsibility).

122. *See* Gutiérrez & Pardo, *supra* note 102, at 200.

importantly for purposes of the lesson plan, the ordinariness of the German soldiers and the officers involved, their junior rank, and First Lieutenant Sibille's principled decision-making likely make it easier for the cadets to identify with the situation in which the company commanders had been placed.[123]

Mindful of the enrichment smart devices can bring to P2P learning,[124] future iterations of *Ordinary Soldiers* should incorporate social media technology and applications in the P2P format. For example, a website that contained video interviews and written resources on leadership, ethics, history, and legal matters could be accessed by the students after the historical presentation to deepen their understanding of relationships between these topics. The small group facilitation training could use video teleconferencing so that remotely located experts or military leaders would be able to convey to the students the importance of understanding and using small group dynamics in their coming military careers. During the first hour of the capstone exercise, students could use their smart phones to send and receive tweets about important or interesting points that had been raised at their respective tables, thereby accelerating the normalizing of the entire group's information. The scribes could blog about their table's results and progress in real time. In the second hour, instant audience survey techniques could be used to quickly assess whether students had in fact understood certain important points of the lesson when they are briefing their results back to the entire group. Incorporating these techniques would not be mere electronic gimmickry. Rather, it would replicate in many ways the communication environment within which these students are accustomed to working, and which they will bring with them into their new jobs as junior military leaders.

---

123. *See* David Boud, *Conclusion* to PEER LEARNING IN HIGHER EDUCATION, *supra* note 121, at 175 (explaining that one of the most fundamental questions that is positively addressed in P2P learning is "how do we learn from those with whom we do not identify?").

124. SIDDIQUE ET AL., *supra* note 120, at 3.

VI. CONCLUSION

As noted at the outset, this article is in part speculative, and based on extrapolations of current trends in the military use and development of cyberspace that might not come to fruition. If these trends were to result in the ability to conduct cyber war in the sense that we ordinarily think about war, however, the long lead times necessary to develop the human capital necessary for ethical and legal decision making in this conflict context mean that we must start building ethical cyber commanders today, from the ground up. Given the likely speed at which future cyber operations would occur, not only will commanders need to accelerate their decision making, but they will also likely need to use ADPs as part of their arsenal in order to maintain their operational effectiveness. The ethical and legal challenges posed by reliance upon this sort of technology must be explored fully to ensure that possible solutions are consistent with the overarching social, political and legal norms we expect our military personnel to meet as they conduct operations on our behalf. Building the ethical cyber commander, and identifying the ethical considerations that will be embedded in her education and training as well as her terms of reference in conducting and planning operations, should be no less important to Information Age societies and their militaries than the development of the weapons cyber commanders might someday use.

This means that merely adjusting programs and methods of instruction and course content will not work – efforts in these areas will require profound rethinking and experimentation before they could become truly effective. These undertakings would require both courage and vision on the part of militaries, because in very meaningful ways, emphasizing techniques such as P2P training enhanced through social media challenge traditional notions of order, control and identity in military organizations.[125] As

125. Robinson, *supra* note 2, at 9 (explaining that critical assessment of military orders by individual subordinates are generally neither valued in military operations and organizations, nor taught in military educational programs).

challenging as this could be, it potentially pales in comparison with what might actually be a more complex problem – educating and training civilian leaders in the ethical and legal use of armed force in cyberspace. Because of the historical nature of the *Ordinary Soldiers* case study, and the relatively uncluttered operational context within which the company commanders of 1st Battalion made their decisions during those fateful few days in October 1941, the lesson plan lends itself to effective discussion with civilian audiences with little or no military background outside the information provided in the case study. Coupled with its delivery in a format both mediated by social media and analogous to the modern information exchange environment, this simplicity lends itself to effective ethical and legal learning for diverse groups of students in learning to negotiate the issues raised by the use of force in this new and evolving forum of human interaction.