THE LAW OF ARMED CONFLICT AND THE RESPONSIBLE CYBER COMMANDER

Jody M. Prescott*

INTRODUCTION

The rate at which cyberspace has become a global medium of trade, social exchange, and system of delivery for government services is astonishing.[1] Despite cyberspace's peaceful utility, however, its use as a medium of armed conflict is likely inevitable, given the significant military advantages to be gained through levering its reach, carrying capacity, and near light-speed pace of action and effect.[2] Some scholars argue that the problem of cyber armed conflict is largely manufactured and a reflection of inordinate military influence in both governmental and academic thinking on the issue.[3] The efforts of numerous countries across the world to accelerate the development of their military offensive capacities, however, suggest that even if cyber armed conflict has not really happened yet, the capacity to conduct it may exist in the near future.[4] For instance, the U.S.

---

* Senior Fellow, West Point Center for the Rule of Law; Adjunct Professor, University of Vermont Department of Political Science. The opinions in this article are mine alone, and reflect the official positions of no U.S. government organization.

1. *See* THE CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD, 5, 7, 11 (2011) [hereinafter UK CYBER STRATEGY], *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf (reporting on the advances of the U.K. in protecting technological infrastructure).

2. *See generally* Nick Hopkins, *Militarisation of Cyberspace: How the Global Power Struggle Moved Online*, GUARDIAN (Apr. 16, 2012, 10:00 AM), http://www.theguardian.com/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle?guni=Article:in%20body%20link (arguing that global reliance on cyberspace provides opportunities for criminal and military activities).

3. MARY ELLEN O'CONNELL ET AL., CYBER SECURITY AND INTERNATIONAL LAW 3, 6 (2012) *available at* http://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf (arguing that we "invent[ed] a cyber war problem" because academics in the early days of international cyber legal scholarship had connections to the military and strongly conditioned the next decade of legal analysis to focus on rare examples of state-sponsored cyber crime, instead of the "real world problems of cyber insecurity, crime and espionage").

4. *See, e.g.*, Andrea Shalal-Esa, *Six U.S. Air Force Cyber Capabilities Designated "Weapons"*, REUTERS (Apr. 9, 2013, 2:46 AM), http://uk.reuters.com/article/2013/04/09/us-cyber-airforce-weapons-idUKBRE93801B20130409 (reporting on tools available to the U.S. Air Force to protect against cyber-warfare); Ellen Nakashima, *Pentagon to Boost Cybersecurity Force*, WASH. POST, Jan. 27, 2013, http://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/19/d87d9dc2-5fec-11e2-b05a-605528f6b712_story_1.html (discussing that the U.S. military plans major increases in cyber personnel recruitment and offensive cyber capability investment); Nick Hopkins, *UK Developing Cyber-weapons Programme to Counter Cyber War Threat*,

Department of Defense (DoD) recently unveiled "Plan X," a large-scale research program geared towards developing cyber weapons and supporting technologies on an industrial scale.[5] Accordingly, to promote predictability in cyberspace's use and to avoid conflict, it is imperative that both state and non-state actors agree on standards of behavior regulating cyber-armed conflict.[6]

Currently, there is a lack of definitive consensus in the international community regarding the rules that apply to military action in cyberspace, especially the law of armed conflict (LOAC).[7] The reasons for this uncertainty are likely threefold. First, powerful cyber state actors fundamentally disagree about what their role in cyberspace should be.[8] Second, envisioning how military action in cyberspace would actually be conducted is difficult because it is so different from the geophysical world.[9] Third, the work that has occurred within and between national governments to better define their understandings of the rules applicable to cyberspace is often classified.[10] The combined effects of these factors have led to, among other things, a lack of clarity as to the rules that apply to cyber armed conflict. Additionally, it has made the military inattentive to the holism that

---

GUARDIAN (May 30, 2011, 4:44 PM), http://www.guardian.co.uk/uk/2011/may/30/military-cyberwar-offensive.

5. *See* Matthew Cox, *DARPA Outlines Plans To Develop Cyber Weapons*, DOD BUZZ (Apr. 25, 2013, 12:05 AM), http://www.dodbuzz.com/2013/04/25/darpa-outlines-plans-to-develop-cyber-weapons (describing "Plan X" creators' efforts to standardize cyber weapons to make them more efficient and predictable); *Special Notice, Plan X Proposers' Day Workshop*, DEF. ADVANCED RES. PROJECTS AGENCY (Aug. 17, 2012), https://www.fbo.gov/index?s=opportunity&mode=form&id=19cced1c188775a844f889872c64c30f&tab=core&_cview=1 [hereinafter Plan X] ("The objective of the Plan X program is to create revolutionary technologies for understanding, planning, and managing cyberwarfare in real-time, large-scale, and dynamic network environments.").

6. Jody M. Prescott, *War by Analogy: US Cyberspace Strategy and International Humanitarian Law*, 156 RUSI J., Dec. 2011, at 38 [hereinafter Prescott, *War by Analogy*] (arguing that the U.S. needs to develop a policy consistent with international humanitarian law to operate in cyberspace).

7. *Cf.* Harold Hongju Koh, *Remarks: Twenty-First-Century International Lawmaking*, 101 GEO. L. J. 725, 742–43 (2013) (debating the need for additional laws governing cyber war).

8. *See* Robert M. McDowell, *A U.N. Regulated Internet? The Case for Defending Against Persistent Intergovernmental Threats to Internet Freedom*, 13 ENGAGE: THE J. OF THE FEDERALIST SOC'Y PRAC. GROUPS 104, 105–06 (2012) (stating that China, Russia, and other nations favor increased governmental regulation of cyberspace to protect sovereignty, security, and territorial integrity).

9. *See* Lior Tabansky, *Basic Concepts in Cyber Warfare*, 3 MIL. AND STRATEGIC AFF., May 2011, at 76–78, *available at* http://www.inss.org.il.cdn.reblaze.com/upload/%28FILE%291308129610.pdf (describing the differences between the geophysical world and "cyberspace").

10. Warren Strobel & Deborah Charles, *With Troops and Techies, U.S. Prepares for Cyber Warfare*, REUTERS BUS. & FIN. NEWS, (June 7, 2013, 3:11 AM), http://www.reuters.com/article/2013/06/07/us-usa-cyberwar-idUSBRE95608D20130607 (stating that new Pentagon rules of engagement are classified and have been finalized).

in which it would rather, for its own reasons, apply domestic-security law and potentially exploit military advantage.[31]

1. The United Kingdom

In November 2011, the British Government published its second cyber strategy (the first was in 2009).[32] Although the *UK Cyber Strategy* does not explicitly mention LOAC, it does establish the British position "that all governments must act proportionately in cyberspace and in accordance with national and international law. This includes respect for intellectual property and for fundamental human rights to freedom of expression and association."[33] Perhaps the *UK Cyber Strategy's* most important contribution to the international discussion on cyberspace is its realistic and explicit recognition of the ambiguity in the current state of the law on cyber conflict, which likely poses the greatest risk for misunderstandings and unnecessary conflicts.[34] The *UK Cyber Strategy* notes that "[t]he blurring of boundaries in cyberspace increases the risk of actions affecting larger numbers of people and organizations unintentionally. At its most serious, this leads to the potential for unpredictable and large-scale shocks."[35] Accordingly, the United Kingdom has committed itself to working "with other countries on practical confidence-building measures to reduce the risk of escalation and avoid misunderstandings."[36]

In the military context, the UK Joint Cyber Unit is "developing new tactics, techniques and plans to deliver military capabilities to confront high-end threats."[37] The British Ministry of Defence (MoD) has confirmed that LOAC applies to cyber operations, but has also stated that "[a]t this stage we have not sought to develop specific rules of engagement for cyber," but that as "our understanding of cyber operations, their potential, their capabilities and the associated norms of behaviour develop and evolve," it might revisit that issue and "possibly devis[e] specific rules of

---

31. UNIV. OF CAL. INST. ON GLOBAL CONFLICT AND COOPERATION, CHINA AND CYBERSECURITY: POLITICAL, ECONOMIC, AND STRATEGIC DIMENSIONS 18–19 (2012), *available at* http://igcc.ucsd.edu/assets/001/503568.pdf (noting that China has a long history of emphasizing "information in warfare" and that Chinese strategists' views on information differ from Americans).

32. UK CYBER STRATEGY, *supra* note 1.

33. *Id*. at 27.

34. *Id.* ¶ 4.16, at 27.

35. *Id*. at 17.

36. *Id.* at 26.

37. Francis Maude, Written Ministerial Statement, Minister for the Cabinet Office and Paymaster General: Progress on the UK Cyber Strategy: Protecting and Promoting the UK in a Digital World 2 (Dec. 3, 2012), *available at* http://www.parliament.uk/documents/commons-vote-office/December_2012/03-12-12/3-Cabinet-Office-UK-Cyber-Security-Strategy.pdf.

dominant personality types were ISTJ (24.7%) and ESTJ (17.7%).[255] One study of senior U.S. military executives, both military and civilian, found the ISTJ type to occur between 19-23%, and the ESTJ type between 12.5-14%.[256] The ISTJ type was dominant for men, but there was a more even distribution of preferred types among women.[257] At the highest levels of senior military U.S. Army leadership, approximately 30% display the ISTJ type,[258] while this type hardly registers among hackers.[259] Even in the one area of commonality between military leadership and hackers, the spike in INTJ personality type frequency relative to the general population, the groups are markedly different.[260] The INTJ rate for military officers in the 2005 study was 13.7%, a six-fold increase over that expected in the general public but less than half the rate found among hackers.[261] Further, the perfectionist INTP hacker has little in common with the decisive, directive ESTJ officer.[262] This suggests that current military personnel policies are biased towards producing senior commanders who are quite unlike the typical hacker.

From a different perspective, however, if cyber military operations are really so markedly different from those in the geophysical world, perhaps the typical, traditional officer is not well suited to be a cyber commander. For example, the common spike in INTJ types suggests hackers and military officers are actually more akin to each other than the general population.[263] Further, mature hackers often enter jobs where they are in fact protecting governmental and commercial entities from cyber intrusions in conformance with the law.[264] INTP hackers and their kindred INTJ types

---

255. *Id*. at 55. MBTI surveys in 1999 and 2000 among primarily mid-career U.S. Marine Corps officers found similar results: INTP (5%), INTJ (8%), ESTJ (17%), and ISTJ (26%). Jane M. Moraski, Leadership: The Personality Factor, Appendix B, 53 (Apr. 2001) (unpublished Masters Thesis, U.S. Marine Corps Command and Staff College) (citing MBTI results from the classes of 1999 and 2000 at the U.S. Marine Corps Command and Staff College, Quantico, Virginia), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA401567 (last visited Nov. 10, 2013).

256. Dianna Lea Williams, *Frequencies of Myers Briggs Type Indicator (MBTI) Among Military Leaders*, 5 J. LEADERSHIP STUD., 50, 52–53 (1998).

257. *Id*. at 55.

258. Peggy C. Combs, US Army Cultural Obstacles To Transformational Leadership 9 (Aug. 30, 2013) (unpublished Masters Degree Research Project, U.S. Army War College), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA469199.

259. *Poll:Hacker News (Myers-Briggs) Personality Types*, *supra* note 248.

260. *Compare Poll:Hacker News (Myers-Briggs) Personality Types*, *supra* note 248, *with* Garren *supra* note 252, at 55 (finding 13.7% of those surveyed were INTJ whereas 2.1% of the U.S. population is INTJ).

261. Garren *supra* note 252, at 53.

262. *Compare Results of Yesterday's Personality Poll: We're Strange*, *supra* note 248, *with* Garren, *supra* note 252, at 55.

263. *Id.*

264. PBS, *supra* note 242.