THE CYBERENEMY: USING THE MILITARY JUSTICE SYSTEM TO PROSECUTE ORGANIZED COMPUTER ATTACKERS

Michael J. Lebowitz†

TABLE OF CONTENTS

† Michael J. Lebowitz, B.A., Kent State University; J.D., Case Western Reserve University School of Law. Currently serves as a war crimes prosecutor in the Office of Military Commissions. He is an Assistant Trial Counsel in the joint, capital war crimes case against five men accused of plotting the 9/11 attacks (United States v. Khalid Sheikh Mohammad, et al.). He previously served as chief legal assistance attorney and military defense counsel in the Virginia Army National Guard as part of the U.S. Army Judge Advocate General's Corps. In addition, he was deployed to Iraq from 2005–2006 as a paratrooper with the Pathfinder Company of the 101st Airborne Division. Mr. Lebowitz has also served as a litigation attorney and military defense counsel in private practice.

I. INTRODUCTION

The United States is literally under cyberassault on a second-by-second basis. These attacks do not captivate the nation through the boom of military ordinance or crackle of gunfire. But it is precisely the silent and unassuming nature that is perhaps the most alarming.[1] Cyberattacks are conducted for many reasons.[2] For some, the attacks are conducted for sport, espionage, or financial gain. Others engage in attacks to achieve much more sinister goals.[3] In response, the United States continues to defend itself against cyberattacks directed at U.S. electronic infrastructure.[4] Numerous experts predict that one day a significant cyberattack will succeed in crashing the U.S. electrical grid, shut down Department of Defense (DoD) communications, or worse.[5]

---

1. *See, e.g.*, William J. Lynn III, *The Pentagon's Cyberstrategy, One Year Later*, FOREIGN AFFAIRS (Sept. 28, 2011), http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later ("For almost all of human history, man has waged war on land and at sea. Air and space emerged as potential battlefields only in the past few generations. Now, the danger of cyberwarfare rivals that of traditional war. The advent of more destructive technologies—and of their inevitable proliferation among actors willing to use them—means that the United States must strengthen its critical national networks against ever worse threats.").

2. A Department of State report relating to cyberattacks described the issue as follows:

> Computer network attacks (CNA), or "cyberattacks," disrupt the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output. Computer hackers opportunistically scan the Internet looking for computer systems that are mis-configured or lacking necessary security software. Once infected with malicious code, a computer can be remotely controlled by a hacker who may, via the Internet, send commands to spy on the contents of that computer or attack and disrupt other computers. Cyberattacks usually require that the targeted computer have some pre-existing system flaw, such as a software error, a lack of antivirus protection, or a faulty system configuration, for the malicious code to exploit. However, as technology evolves, this distinguishing requirement of CNA may begin to fade. For example, some forms of [electronic attack] can now cause effects nearly identical to some forms of CNA. For example, at controlled power levels, the transmissions between targeted microwave radio towers can be hijacked and specially designed viruses, or altered code, can be inserted directly into the adversary's digital network.

CLAY WILSON, COMPUTER ATTACK AND CYBERTERRORISM: VULNERABILITIES AND POLICY ISSUES FOR CONGRESS 5 (2005), *available at* http://fpc.state.gov/documents/organization/45184.pdf.

3. For example, "cyberterrorism" is defined by the Federal Emergency Management Agency as "unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives." *Id.* at 6; *see* Dorothy E. Denning, *Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, *in* NETWORKS AND NETWARS: THE FUTURE OF TERROR, CRIME, AND MILITANCY 239, 241 (John Arquilla & David Ronfeldt eds., 2001) [hereinafter Denning, *Activism*] (defining cyberterrorism as the "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage"); *see also* Dorothy E. Denning, *Is Cyber Terror Next?*, SOC. SCI. RES. COUNCIL (Nov. 1, 2001), http://www.ssrc.org/sept11/essays/denning.htm (explaining that computer attacks by cyberterrorists can lead to death, injury, extended power outages, airplane crashes, water contamination, or major loss of confidence for portions of the economy).

4. *See* WILSON, *supra* note 2, at 6 ("[Department of Homeland Security] officials have also asserted that cybersecurity cuts across all aspects of critical infrastructure protection and that cyberoperations cannot be separated from the physical aspects of businesses because they operate interdependently."); *see also* Pub. Citizen v. Nuclear Regulatory Comm'n, 573 F.3d 916, 921 n.4 (9th Cir. 2009) (reflecting that the NRC was instructed by Congress to consider an assessment of "physical, cyber, biochemical, and other terrorist threats," along with eleven additional more conventional attacks).

5. Rep. Cliff Stearns (R-Fla.), the chairman of the Energy and Commerce Oversight and Investigations subcommittee, in expressing Congressional concerns, made the following statement at a Congressional hearing:

> Ask any expert in the national security field and see what keeps them up at night. They would probably tell you, as they tell me, that it is the increased possibility of a devastating cyber attack . . . . Imagine the impact of a cyber attack to the electrical grid: How many days could

However, the burgeoning field of cyberforensics continues to develop.[6] Cyberattackers have been very successful to date in creating veritable mazes connected to random points around the world to avoid detection.[7] Cyberforensics provides the technical ability to navigate the maze and ultimately trace a cyberattack back to its source.[8] Just as experts predict the eventual success of a significant cyberattack, experts also predict that one day cyberforensics will lead to the identity and possible capture of a significant cyberattacker.[9]

If the cyberattacker is indeed knowingly working in conjunction with an organized enemy group hostile to the United States, the cyberattacker may fall into a specific class of detainee referred to in this Article as a cyberenemy. When the day comes where a significant cyberenemy is captured, the United States may be forced to make a choice: treat the accused cyberenemy as a common criminal or regard this individual as someone engaged in war or hostilities against the United States.[10] If the government opts to treat the accused cyberenemy as a common criminal, then the detainee may be prosecuted in federal court. But if the individual is deemed to be truly engaged in hostilities toward the United States, Congress—coupled with executive orders relating to the Manual for Courts-Martial (MCM)—has authorized in certain cases the offense and jurisdiction to prosecute a cyberenemy within the

---

> hospitals operate with on-site electricity generation? How would metro rail systems operate, if at all? How would we recharge our smartphones or access the Internet?

Brendan Sasso, *Lawmakers Fear Power Grid Could Fall to Cyber Attack*, HILLICON VALLEY (Feb. 28, 2012, 12:03 PM), http://thehill.com/blogs/hillicon-valley/technology/213015-lawmakers-worry-about-cyber-attacks-on-electrical-grid.

6. *See, e.g.*, Alexis C. Madgrigal, *The Stuxnet Worm? More than 30 People Built It*, ATLANTIC (Nov. 4, 2010), http://www.theatlantic.com/technology/archive/2010/11/the-stuxnet-worm-more-than-30-people-built-it/66156/ (detailing how a security firm reverse engineered the Stuxnet computer virus and found traces of more than thirty programmers within the source code).

7. *Research Shows 'Dramatic Growth' in Global Cyber Attacks*, INFOSECURITY (Feb. 13, 2013), http://www.infosecurity-magazine.com/view/30736/research-shows-dramatic-growth-in-global-cyber-attacks/.

8. Michael Vatis, *Can the U.S. Investigate a Cyber Attack?*, COMPUTER CRIME RES. CENTER, http://www.crime-research.org/library/Vatis2.htm (last visited Feb. 15, 2013) (citing a Dartmouth report identifying areas of improvement for cyberattack investigation including preliminary data collection, log analysis, Internet protocol tracing, information sharing, and maintaining high-levels of technical skill among investigators).

9. Investigators from Interpol and other international law enforcement agencies are becoming more successful in identifying suspected members of sophisticated cyberattack groups. *See, e.g.*, *Update 1- Spain, South America Arrest 25 in Hacking Probe*, REUTERS (Feb. 28, 2012), http://www.reuters.com/article/2012/02/28/spain-cyber-arrests-idUSL5E8DS80W20120228 (detailing the arrest of twenty-five members of Anonymous); *see also* Pete Yost, *14 Arrested for Alleged Cyberattack on Pay Pal*, ASSOCIATED PRESS (July 19, 2011, 11:49 PM), http://www.usatoday.com/tech/news/2011-07-19-paypal-anonymous-wikileaks-arrests_n.htm (detailing the arrests of members of LulzSec).

10. *See* Susan W. Brenner, *Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law*, MURDOCH U. ELECTRONIC J. L., June 2001, at ¶ 10 (warning that the cybercrime situation is such that "each nation must examine its own penal and procedural law to determine whether they are adequate for dealing with the so-far-identified varieties of cybercrimes"), *available at* http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html. Brenner identifies cybercrimes against the state as acts specifically directed at:

> Destroying the viability of the State (e.g., treason and sabotage), acts undertaken to weaken the effectiveness of the State (e.g., espionage, the internal dissemination of misinformation and propaganda, rioting), acts targeting various state infrastructures (e.g., terrorism directed at transportation systems, economic systems, public utilities, medical systems, etc.), acts taken to undermine the State's fiscal stability (e.g., counterfeiting), and the like.

Id. at ¶ 53.

military justice system.[11]

This Article proposes a method for prosecuting captured cyberenemies within the military justice system. This Article will begin by expounding upon the technology involved and the U.S. view of hostilities relating to cyberattacks. The following section relates to the limited authorization for applying the Uniform Code of Military Justice (UCMJ) Article 104 to non-U.S. servicemembers within the courts-martial context. This Article then considers jurisdiction for prosecuting cyberenemies by military commission.

II. CYBERTHREATS

A. Scope of Attacks

In early 2012, a high-ranking Venezuelan diplomat based in Miami was implicated in a cyberattack plot against the United States.[12] Besides Venezuela, the plot purportedly involved Cuba and Iran.[13] The ruling regimes of those countries certainly demonstrate varying levels of hostility to the United States. At roughly the same time in early 2012, organized and coordinated cyberattack efforts directed toward the United States reportedly emanate from China and Russia.[14] In addition, organized groups of non-state actors also have directed attacks toward U.S. cyberinfrastructure. Such cyberattacks can come in numerous forms. For example, Al Qaeda operative Mohammed Salahi reportedly was involved in the planning of a denial of service computer attack.[15] Keylogger attacks through malicious codes and computer infections have stolen data while also disrupting businesses and

11. 10 U.S.C. § 904 (2006) (corresponds to U.C.M.J. art. 104 (2010)), *reprinted in* MANUAL FOR COURTS-MARTIAL: UNITED STATES pt. 4, at 41–42 (2012) [hereinafter MCM]; 2011 Amendments to the Manual for Courts-Martial, United States, 76 Fed. Reg. 78,451 (Dec. 16, 2011).

12. *US Expels Venezuelan Diplomat Who 'Discussed Cyber War on America,'* GUARDIAN (Jan. 8, 2012, 10:40 PM), http://www.guardian.co.uk/world/2012/jan/09/us-expels-venezuelan-diplomat-cyber.

13. *Id*.

14. *See* RYAN SHERSTOBITOFF, ANALYZING PROJECT BLITZKRIEG, A CREDIBLE THREAT 3 (2012), *available at* http://www.mcafee.com/us/resources/white-papers/wp-analyzing-project-blitzkrieg.pdf (explaining research into the credibility and authenticity of a Russian cyberattack on U.S. financial institutions). A report by the United States-China Economic and Security Review Commission (USCC) discussed the Chinese People's Liberation Army's (PLA) development of advanced cyberwarfare capabilities. *See* BRYAN KREKEL, US-CHINA ECON. & SEC. REVIEW COMM'N, CAPABILITIES OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION 6 (2009) ("Increasingly, Chinese military strategists have come to view information dominance as the precursor for overall success in a conflict. The growing importance of [information warfare] to [the PLA] is also driving it to develop more comprehensive computer network exploitation (CNE) techniques to support strategic intelligence collection objectives and to lay the foundation for success in potential future conflicts."), *available at* http://cdm266901.cdmhost.com/cdm/singleitem/collection/p266901coll4/id/3130/rec/12. The PLA has created special computer network attack and exploitation units using civilian as well as military personnel, the report noted. *Id.* at 7. These units are engaged in a long-term, sophisticated computer network exploitation campaign against Western targets. *Id.*

15. *See* Salahi v. Obama, 625 F.3d 745, 749–50 (D.C. Cir. 2010) (acknowledging in a habeas corpus case that alleged Al Qaeda operative "knew about and had some involvement in planning for denial of service computer attacks"); *see also Interview: Richard Clarke*, FRONTLINE (Mar. 18, 2003), http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/clarke.html (noting that seized computers belonging to Al Qaeda indicate that its members were becoming familiar with hacker tools that are freely available over the Internet).

government systems.[16]

Such attacks also are capable of expanding beyond computer systems and into the physical world.[17] In Illinois, a feared cyberattack from Russia was initially believed to have caused a water treatment plant to spin out of control.[18] A virus similar to the Stuxnet attack on Iranian nuclear development also has the capability to cause widespread equipment and power failures.[19] Once computers are infected, enemy operatives can remotely engage in espionage while also taking out command-and-control capabilities and financial interests.[20] Death and destruction among military personnel and civilians could result if a serious attack succeeds.[21] In short, attacks initiated by organized groups hostile to the United States can use cyberattacks against defense, governmental, and business targets that achieve similar tactical results as those effectuated by conventional warfare.[22]

---

16. *See, e.g.*, Patco Const. Co. v. People's United Bank, 684 F.3d 197, 210 n.8 (1st Cir. 2012) (describing keylogger attacks as "a form of computer malware, or malicious code, capable of infecting a user's system, secretly monitoring the user's Internet activity, recognizing when the user has browsed to the website of a financial institution, and recording the user's key strokes on that website").

17. Reports of computer attacks transcending into the physical realm reportedly occurred during the Cold War. One account is as follows:

> According to news sources, in the 1980s during the Cold War, the United States CIA deliberately created faulty SCADA software and then planted it in locations where agents from the Soviet Union would steal it. Unknown to the Soviets, the SCADA software, which was supposedly designed to automate controls for gas pipelines, was also infected with a secret Trojan Horse programmed to reset pump speeds and valve settings that would create pressures far beyond what was acceptable to pipeline joints and welds. The result, in June 1982, was a monumental nonnuclear explosion on the trans-Siberian gas pipeline, equivalent to 3 kilotons of TNT. However, the event remained secret because the explosion took place in the Siberian wilderness, and there were no known casualties.

WILSON, *supra* note 2, at 29; *see also* William Safire, Opinion, *The Farewell Dossier*, N.Y. TIMES, Feb. 2, 2004, http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html (noting that NORAD monitors first suspected that the explosion was nuclear but that satellites did not pick up an electromagnetic pulse that would have accompanied a nuclear detonation).

18. Ellen Nakashima, *Water-Pump Failure in Illinois Wasn't Cyberattack After All*, WASH. POST (Nov. 25, 2011), http://www.washingtonpost.com/world/national-security/water-pump-failure-in-illinois-wasnt-cyberattack-after-all/2011/11/25/gIQACgTewN_story.html.

19. William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0; *see also Cyberwar: Pentagon Takes on Cyber Enemies, Other Agencies*, DEF. INDUS. DAILY (Nov. 8, 2011), http://www.defenseindustrydaily.com/cyberwar-department-defense-doctrine-response-06931/ [hereinafter *Cyberwar*] ("Although Stuxnet appears to have been developed to attack Iranian nuclear facilities, it has spread far beyond its intended target. The Stuxnet malware is able to be used against industrial facilities in Western countries, including the United States . . . .").

20. *See Cyberwar*, *supra* note 19 (describing many of the offensive and remote control capabilities of the computer attacks such as Stuxnet). Researchers discovered that the Flame virus was written by different teams of programmers but commissioned by the same larger entity, such as a nation. *Id.* Flame reportedly was used as a reconnaissance tool against Iran and used operationally in conjunction with Stuxnet. Nicole Perlroth, *Researchers Find Clues in Malware*, N.Y. TIMES (May 30, 2012), http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html.

21. *See* Lynn, *supra* note 1 ("[T]he danger of cyberwarfare rivals that of traditional war.").

22. *See, e.g.*, Dan Verton, *Cyber-Terrorism*, COMPUTERWORLD, Aug. 11, 2003, at 36 (noting that cyberterrorism "can . . . take the form of a physical attack . . . that destroys" computerized nodes for critical infrastructures, such as the "Internet, telecommunications, or the electric power" grid, without ever touching a keyboard).

B. Nexus Between Cyberattacks and Hostilities

U.S. institutions are constantly fending off cyberattacks.[23] Relating to these extreme scenarios, the DoD is increasingly beginning to view cyberattacks as hostile actions against the nation.[24] In 2011, a DoD report stated, "[w]hen warranted, we will respond to hostile attacks in cyberspace as we would to any other threat to our country."[25] Hostile acts, the report said, could include "significant cyberattacks directed against the U.S. economy, government, or military."[26] Suggested DoD responses to significant cyberattacks could include "electronic means or more conventional military options."[27] The nexus between significant cyberattacks and a precursor to traditional armed conflict is to the point where one U.S. military official bluntly warned that "[i]f you shut down our power grid, maybe we will put a missile down one of your smokestacks."[28] In addition, the military is expending extensive resources on cracking the anonymous nature of the cyberrealm in an effort to identify individual attackers, as well as the groups they represent.[29] As such, the budding field of cyberforensics is developing on an international scale.[30]

Inevitably, cyberattackers will be identified as operatives of organized groups hostile to the United States.[31] Therefore, these operatives and their overarching organizations will essentially be considered cyberenemies.[32] But

---

23. *See* Jerrold M. Post et al., *From Car Bombs to Logic Bombs: The Growing Threat From Information Terrorism*, 12 TERRORISM & POL. VIOLENCE 97, 97–98 (2000) (describing cyberattacks on various U.S. Internet companies and the DoD).

24. *See We Are Prepared to Take Military Action Against Cyber Attackers, Warns U.S. Defence Chiefs*, MAILONLINE (Nov. 16, 2011), http://www.dailymail.co.uk/news/article-2062247/Cyber-attacks-US-defence-chiefs-prepared-military-action.html [hereinafter *We Are Prepared*] ("Defence chiefs have warned that the United States is prepared to retaliate with military force if it came under cyberattack.").

25. U.S. DEPT. OF DEFENSE, CYBERSPACE POLICY REPORT 2 (2011) (reporting to Congress pursuant to H.R. 6523, 111th Cong. § 934 (2010)), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

26. *Id*. at 4.

27. *We Are Prepared*, *supra* note 24.

28. Siobhan Gorman & Julian E. Barnes, *Cyber Combat: Act of War*, WALL ST. J. (May 30, 2011, 10:30 PM), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html.

29. *We Are Prepared*, *supra* note 24. In an effort to crack the problem of anonymity, the DoD is "supporting innovative research and development . . . focus[ing] on . . . assessing the identity of the attacker via behavior-based algorithms . . . ." U.S. DEPT. OF DEFENSE, *supra* note 25, at 4. The report added that "[t]he Intelligence Community and U.S. Cyber Command continue to develop a highly skilled cadre of forensics experts." *Id.*; *see also* Justin Blum, *FBI Will Increase Efforts to Battle Computer Hacking, Mueller Testifies*, BLOOMBERG (June 8, 2011), http://www.bloomberg.com/news/2011-06-08/fbi-will-focus-on-fighting-computer-hacking-mueller-says.html (stating that the FBI will put increased emphasis on all variations of cyberthreats).

30. *See supra* note 6 and accompanying text.

31. *See, e.g.*, WILSON, *supra* note 2, at 7 (suggesting cyberterrorism may be "the use of computers as weapons, or as targets, by politically motivated international, or sub-national groups, or clandestine agents who threaten or cause violence and fear in order to influence an audience, or cause a government to change its policies").

32. *See id.* at 23 ("Potentially severe cyberattack tools may be first developed and then secretly tested by dispersed terrorist groups using small, isolated laboratory networks, thus avoiding detection of any preparation before launching a widespread attack on the Internet."). *See generally* Denning, *Activism*, *supra* note 3, at 285 (explaining that networking technologies, such as the Internet, are advantageous for attackers who are geographically dispersed).

Networking supports redundancy within an organization, and it suggests the use of

what happens if the United States actually catches one of these enemy cyberattackers? The government has yet to develop a policy toward prosecuting a cyberenemy who uses cyberwarfare as the preferred means of attack.[33] Mainly, does the government treat cyberenemies as unconventional combatants relating to hostilities? Or does the government seek to prosecute cyberenemies as common criminals through the federal court system?

III. COURT-MARTIAL

A. UCMJ Article 104 Jurisdiction

The notion of prosecuting domestic and foreign cyberenemies through a military court-martial may initially sound implausible. Certainly, courts-martial jurisdiction is governed by the UCMJ,[34] with structural guidance provided through the MCM.[35] The UCMJ generally applies to servicemembers and accompanying personnel.[36] As such, the punitive articles contained within the UCMJ typically do not apply to foreign agents hostile to the United States or hostile non-servicemember citizens and permanent residents who breach their duty of loyalty to the country. However, since 1950, a seemingly narrow mechanism was created through UCMJ Article 104 that can be used to prosecute alien personnel in either a court-martial or military commission.[37]

The Article 104 mechanism can, in turn, be used to provide a military justice solution for prosecuting certain classes of foreign and even domestic

---

> swarming tactics, new weapons, and other new strategies for conducting conflict that show advantages over traditional government hierarchies. Inflexibility is a major disadvantage when a hierarchy confronts a networked organization. Networks blend offensive and defensive functions, while hierarchies struggle with allocating responsibility for either.

Id.

33. *See* Brenner, *supra* note 10, ¶ 12. After a destructive "love bug" shut down computers from Ford Motor Company, Dow Chemical Company, and the British House of Lords, the investigation led to the Philippines. *Id.* ¶¶ 5–6. But the lack of cybercrime-specific penal laws and/or inadequacy of penal laws that were crafted to deal with such conduct affected the case's prosecution, particularly due to "the difficulty of ascertaining which nation(s) has/have jurisdiction to prosecute a cybercriminal and, once this determination has been made, of asserting jurisdiction over that person . . . ." *Id.* ¶ 8.

34. *See* U.C.M.J. art. 2 (2010) (to be codified at 10 U.S.C. § 802), *reprinted in* MCM, *supra* note 11, app. 2, at 1–2 (identifying which persons are subject to the UCMJ).

35. *See generally* MCM, *supra* note 11 (a guide to the conduct of courts-martial).

36. *See* U.C.M.J. art. 3 (2010) (to be codified at 10 U.S.C. § 803), *reprinted in* MCM, *supra* note 11 app. 2, at 2 (addressing members of the Armed Forces); MCM, *supra* note 11, pt. 1, at 1 ("The purpose of military law is to promote justice, to assist in maintaining good order and discipline in the armed forces, to promote efficiency and effectiveness in the military establishment, and thereby to strengthen the national security of the United States."). *But see* U.C.M.J. art. 18 (2010) (to be codified at 10 U.S.C. § 818), *reprinted in* MCM, *supra* note 11, app. 2, at 6 ("General courts-martial *also have jurisdiction to try any person who by the law of war* is subject to trial by a military tribunal and may adjudge any punishment permitted by the law of war." (emphasis added)).

37. U.C.M.J. art. 104 (2010) (to be codified at 10 U.S.C. § 904), *reprinted in* MCM, *supra* note 11, pt. 4, at 41–42. Article 18 also can provide a narrow jurisdictional avenue for handling specific classes of cyberattacks as law of war violations. *See, e.g.*, David K. Linnan, ENEMY COMBATANTS, TERRORISM, AND ARMED CONFLICT LAW: A GUIDE TO THE ISSUES 128 (2008) (stating that any person, whether or not a member of an armed force, can fall under the "any person" provision of Article 18 if they fall under a very limited category of criminal activity relating to law of war violations).

cyberattackers.[38] This premise was bolstered in the Military Commissions Act of 2009 when Congress specifically authorized that alien unprivileged enemy belligerents could be prosecuted under Article 104, as well as Article 106—relating to the offense of spying.[39] That statement is significant because it offers congressional acceptance to the notion that Articles 104 and 106 can indeed be applied to aliens as opposed to merely U.S. servicemembers.[40]

Article 104 criminalizes "aiding the enemy."[41] This is a potential capital offense relating to individuals who assist enemy organizations through a very broad scope of activities.[42] The wide array of offenses contained within Article 104 includes: direct and indirect acts of communicating with the enemy; giving intelligence to the enemy; assisting the enemy with arms, ammunition, supplies, money, or other things; and harboring or protecting the enemy.[43] In addition, Article 104, as well as Article 106, uniquely attach jurisdiction to "any person" through the UCMJ and the MCM.[44] The MCM further explains that "any person" applies to "*all persons whether or not otherwise subject to military law*. Offenders may be tried by court-martial or by military commission."[45] The jurisdictional application of Article 104 is a significant departure from nearly all other punitive offenses within the UCMJ.[46] Other than the spying offense of Article 106, the UCMJ punitive articles apply only to servicemembers and other narrow groups normally

38. U.C.M.J. art. 104; *see also* U.C.M.J. art. 2(b) (authorizing military jurisdiction to trial by courts-martial for offenses against military law and, in the case of general courts-martial, of persons who by the law of war are subject to trial by military tribunals). In 2012, for example, Jeremy Hammond of Chicago was arrested as part of a concerted cyberattack on business and government entities as retaliation for government and business policies. Also charged in the same wave of attacks were four foreign hackers. Hammond was connected to various international groups, including AntiSec, LulzSec, and Anonymous. Todd Lighty & Wailin Wong, *Chicago Man, 27, Charged in Cyber Attack*, CHI. TRIB. (Mar. 6, 2012), http://articles.chicagotribune.com/2012-03-06/business/chi-chicago-raid-linked-to-hacking-arrests-20120306_1_cyber-attack-lulzsec-antisec. Although this attack did not rise to the level of a significant war crime, it is indicative of the nexus between international and domestic attackers and how upon arrest, each attacker could be subject to military justice. *Id.* These arrests also demonstrate the ability to find and arrest such attackers. *Id.*

39. *See* Military Commissions Act of 2009, Pub. L. No. 111-84, § 1802, 123 Stat. 2574, 2611 (2009) (to be codified at 10 U.S.C. § 950(t)) ("Any person subject to this chapter who, in violation of the law of war and with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign power, collects or attempts to collect information by clandestine means or while acting under false pretenses, for the purpose of conveying such information to an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished by death or such other punishment as a military commission under this chapter may direct.").

40. *Id*.

41. U.C.M.J. art. 104 ("Any person who[:] (1) aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things; or (2) without proper authority, knowingly harbors or protects or gives intelligence to, or communicates or corresponds with or holds any intercourse with the enemy, either directly or indirectly; shall suffer death or such other punishment as a court-martial or military commission may direct.").

42. *Id*.

43. *Id*.

44. *Id.* arts. 104, 106.

45. MCM, *supra* note 11, pt. 4, at 41 (explaining the scope of Article 104) (emphasis added).

46. S*ee* Maj. E. John Gregory, *Trying Unlawful Combatants at General Courts-Martial: Amending the UCMJ in Light of the Military Commissions Experience*, 203 MIL. L. REV, 150, 166 n.70 (2010) (labeling Article 104 as a "possible exception" to the norm that could potentially be used punitively via courts-martial against enemy combatants).

subject to military law.[47] By specifically applying Article 104 to literally any person, the intent of the MCM appears to be to provide military prosecutors with the ability to assert jurisdiction over specific classes of enemy operatives with aiding the enemy through courts-martial.[48] Importantly, perhaps through the standalone jurisdictional language of Article 18 that offers courts-martial jurisdiction to try "any person who by the law of war is subject to trial by a military tribunal," the language of Article 104 and its pertinent executive orders also offer a means for prosecuting certain classes of U.S. civilians by courts-martial rather than federal court.[49]

Congress in 2009 specifically extended jurisdiction of Articles 104 and 106 to alien operatives otherwise subject to military commissions.[50] But in the courts-martial context, it remains an untested question whether the jurisdictional language in Articles 104 and 106 can indeed be extended to non-U.S. servicemembers.[51] Specifically, can the statement, "all persons, whether or not otherwise subject to military law," be construed to overcome jurisdictionally-limiting language of UCMJ Article 2?[52]

Article 2 generally applies to members of the U.S. Armed Forces.[53] But even Article 2 does provide for a military justice solution against non-U.S. servicemembers in some limited circumstances.[54] For example, prisoners of war in custody of the Armed Forces are subscribed jurisdiction.[55] In addition, "in times of declared war or contingency operation, persons serving with or accompanying an armed force in the field" also fall under courts-martial jurisdiction pursuant to Article 2 and likely Article 18.[56] As such, while the jurisdictional exception of Article 104 remains untested in the courts-martial

47. U.C.M.J. art. 106 ("Any person who in time of war is found lurking as a spy or acting as a spy . . . shall be tried by a general court-martial or by a military commission and on conviction shall be punished by death.").

48. Articles 104 and 106 are among the few punitive articles that do not contain jurisdictional language such as "any person subject to this chapter," "any member of the armed forces," or other language requiring specific military status. *See generally id.* arts. 104, 106. Article 2 defines "subject to this chapter" as essentially those with some military connection, including "persons serving with or accompanying an armed force in the field" during wartime. U.C.M.J. art. 2(a)(10) (2010) (to be codified at 10 U.S.C. § 802(a)(10)), *reprinted in* MCM, *supra* note 11, app. 2, at 2. The other exceptions to the jurisdictional language are Article 83—fraudulent enlistment, appointment or separation, and Article 113—misbehavior of sentinel. U.C.M.J. arts. 83, 113 (2010) (to be codified at 10 U.S.C. §§ 883, 913), *reprinted in* MCM, *supra* note 11, pt. 4, at 8–9, 57–59.

49. U.C.M.J. art. 18 (2010) (to be codified at 10 U.S.C. § 818), *reprinted in* MCM, *supra* note 11, app. 2, at 6.

50. *See* Military Commissions Act of 2009, Pub. L. No. 111-84, § 1802, 123 Stat. 2574, 2576 (2009) (to be codified at 10 U.S.C. § 948(d)) (stating that any persons subject to this chapter may be tried by a military commission).

51. *See, e.g.*, Gregory, *supra* note 46, at 166 n.70 (noting that Articles 104 and 106 may serve as exceptions to the jurisdictional limits of clause 2 of the MCM).

52. MCM, *supra* note 11, pt. 4, at 41.

53. U.C.M.J. art. 2 (2010) (to be codified at 10 U.S.C. § 802), *reprinted in* MCM, *supra* note 11, app. 2, at 1 (declaring that this chapter applies to "[m]embers of a regular component of the armed forces").

54. *Id*. art. 2(a)(9)–(10) (applying UCMJ jurisdiction to prisoners of war and persons serving with or accompanying an armed forces member in the field).

55. *Id*.

56. *Id.* arts. 2(a)(10), 18. Article 18 is the modern incarnation of the historic Article of War 12, which granted general court-martial jurisdiction over anyone who violated the law of war. *See* Linnan, *supra* note 37, at 124.

context, the language is not inapposite to prosecutions involving a limited class of non-servicemembers engaged in hostilities against the United States.[57]

Judge Scott W. Stucky of the Court of Appeals for the Armed Forces (CAAF) said in April 2012 that ninety-nine percent of the cases heard by the CAAF involve active duty servicemembers who have been convicted at a court-martial.[58] However, Judge Stucky recognized that there are one percent of cases that do not.[59] The most recent example involved the prosecution of a dual citizen of Iraq and Canada who was employed as an interpreter for U.S. forces in Iraq. That case, *United States v. Ali*, was a direct challenge to the application of Article 2 against a non-servicemember.[60] Although *Ali* did not involve aiding the enemy, it does highlight the willingness of military courts to accept jurisdiction of a limited class of cases against aliens who are not members of the U.S. armed forces.

There is a historic precedent toward prosecuting non-U.S. servicemembers by courts-martial. The intermediate appellate court in *Ali* noted that "all grants of jurisdiction to military courts found in the [UCMJ] must be enforced . . . unless we are convinced that they are fundamentally hostile to military due process, or that they have been specifically condemned by the Supreme Court."[61] The Supreme Court has, for example, generally prohibited the use of military commissions against U.S. citizens.[62] But the Supreme Court has specifically upheld the general notion of permitting courts-martial against non-U.S. servicemembers.[63] "This recognition by the Supreme Court of the historical use of military courts to try civilians in areas of actual fighting, coupled with the recognition of the broad authority of military commanders on the battlefront would seem to authorize, or at least not prohibit, the exercise of military jurisdiction" over an alien, non-servicemember.[64] This precedent further provides a basis for subscribing jurisdiction to a limited class of cyberattackers based on the language of Article 104 and the MCM, perhaps through the jurisdictional language of Article 18 pertaining to "any person who by the law of war" in non-capital cases, even if the language of Article 2 does not cleanly apply.[65]

---

57. U.C.M.J. art. 2.

58. Mike Hanzel, *CAAF Outreach Argument in Seattle:* United States v. Ali, *No. 12-0008/AR*, CAAFLOG (Apr. 6, 2012), http://www.caaflog.com/2012/04/06/caaf-outreach-argument-in-seattle-united-states-v-ali-no-12-0008ar/.

59. *Id*.

60. *See* United States v. Ali, 70 M.J. 514, 515 (A. Ct. Crim. App. 2011) ("[A]ppellant filed a petition [arguing] that his court-martial lacked jurisdiction.").

61. *Id.* at 520 (quoting United States v. Burney, 21 C.M.R. 98, 104–05 (C.M.A. 1956)).

62. *See Ex parte* Milligan, 71 U.S. (4 Wall.) 2, 45 (1866) ("It is evident, therefore, that by no loose and general construction of the law can citizens be held amenable to military tribunals."); *see also* United States *ex. rel.* Toth v. Quarles, 350 U.S. 11, 13–15 (1955) (prohibiting use of military courts to try former service members who had severed all relationship with the military at time of trial).

63. *See* Reid v. Covert, 354 U.S. 1, 33 (1957) ("In the face of an actively hostile enemy, military commanders necessarily have broad power over persons on the battlefront.").

64. *Ali*, 70 M.J. at 519–20.

65. U.C.M.J. art. 18 (2010) (to be codified at 10 U.S.C. § 818), *reprinted in* MCM, *supra* note 11, app. 2, at 6. The Article 104 language referring to "whether or not otherwise subject to military law" is important because it can serve as an exception to typical precedent requiring some status by the offender to "military law." *See* Willenbring v. Neurauter, 48 M.J. 152, 158 (C.A.A.F. 1998) ("A discharge or other separation from

Importantly, the MCM under Article 106 elaborates upon the meaning of the term "any person" in a section pertaining to the scope of the offense.[66] The MCM states, "[t]he words 'any person' bring within the jurisdiction of general courts-martial and military commissions all persons of whatever nationality or status who commit spying."[67] The MCM does not contain this language within the scope of the offense section of Article 104. Instead, the scope of Article 104 "denounces offenses by all persons whether or not subject to military law. Offenders may be tried by court-martial or by military commission."[68] The MCM's plain language of Article 106 specifically asserts courts-martial and military commission jurisdiction to aliens.[69] The MCM's language of Article 104 follows along the same broad scope, albeit with different wording.[70] As such, the MCM advises that Articles 104 and 106 can conceivably be used in a prosecution against certain classes of cyberenemies.[71]

B. "Enemy" Requirement

The "any person" language in Article 104 offers authorization for jurisdiction of an individual engaged in significant acts of cyberattacks or cyberterrorism.[72] But Article 104 also requires that such an individual must be actually aiding an "enemy."[73] The MCM defines the enemy as follows:

> "Enemy" includes organized forces of the enemy in time of war, any hostile body that our forces may be opposing, such as a rebellious mob or band of renegades, and includes civilians as well as members of military organizations. "Enemy" is not restricted to the enemy government or its armed forces.[74]

Applying this definition of the enemy to Article 104, the notion of prosecuting certain classes of cyberattackers as "cyberenemies" becomes a bit more plausible. For example, terrorist groups such as Al Qaeda or Hezbollah can be regarded as organized hostile bodies.[75] Likewise, loosely-connected

---

military service, however, does not preclude trial by court-martial, as a matter of constitutional law, if, at the time military jurisdiction is exercised, the individual is still a member of the armed forces or is otherwise in a status subject to military law"). If "military law" jurisdiction is based on Article 2 and Article 3 of the UCMJ, then Articles 104 and 106 provide an exception within the Manual for Courts-Martial. *See* U.C.M.J. art. 18 (detailing over whom the general courts-martial have jurisdiction).

66. *See* MCM, *supra* note 11, pt. 4, at 43–44 (defining "any person" in the context of espionage).

67. *Id*.

68. *Id*. pt. 4, at 41.

69. *See id*. pt. 4, at 43–44 (giving "any person" a broad scope of "all persons of whatever nationality or status").

70. *See id*. pt. 4, at 41 (containing the same broad "any person" language, albeit without the explanation of the term as found in Article 106).

71. *Id*. pt. 4, at 41, 43–44.

72. *Id*. pt. 4, at 41; *see also* U.C.M.J. art. 21 (2010) (to be codified at 10 U.S.C. § 821), *reprinted in* MCM, *supra* note 11, app. 2, at 6 (explaining the congressional notice of the law of war: "[t]he provisions of this chapter conferring jurisdiction upon courts-martial do not deprive military commissions, provost courts, or other military tribunals of concurrent jurisdiction with respect to offenders or offenses that by statute or by the law of war may be tried by military commissions, provost courts, or other military tribunals").

73. MCM, *supra* note 11, pt. 4, at 41.

74. *Id*. pt. 4, at 34.

75. *See* Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001) (authorizing the use of military force relating to Al Qaeda, the Taliban, and associated forces); *see also Assessing the*

cyberattackers intent on raising chaos or political retribution against the United States certainly can be viewed as a band of renegades while operating under a recognizable banner.[76] A cybercriminal brand called "Anonymous" is one such example, although that organization seemingly has not yet crossed the line from criminality to actual cyberwarfare.[77] It also can be argued that the United States is opposing these groups based on the significant resources expended to defend U.S. electronic systems from attack, along with additional efforts for potential offensive operations.[78] Therefore, Article 104 through statute and the MCM provides the jurisdictional and punitive means to bring a military justice solution to any individual operative caught assisting such groups in cyberattacks.[79]

Along similar lines, operatives from foreign militaries or intelligence agencies also could be subject to Article 104 when engaged in significant cyberattacks.[80] In addition, individuals contracted out by foreign government or paramilitary arms also would be considered to be aiding the enemy under Article 104.[81] The notion of bringing such contractors to justice via courts-martial is not without precedent. In the nineteenth century, for example, Congress authorized naval courts-martial against privateers.[82]

C. Assessing the "Enemy" as a "Hostile Body"

Relating to the modern phenomenon of cyberattackers, Article 104 and the MCM establish jurisdiction and the offenses.[83] The final aspect for determining whether the overarching group associated with the individual offender is the enemy as applied to Article 104, is consideration of the issue of

---

Strength of Hezbollah: Hearing Before the Subcomm. on Near Eastern and South and Central Asian Affairs of the S. Comm.. on Foreign Relations, 111th Cong. 6 (2010) [hereinafter *Assessing the Strength of Hezbollah*] (reaffirming Hezbollah's status as a terrorist organization and adding that the "United States continues to take the threats posed by Hizballah to the United States, to Lebanon, to Israel, and the region at large, with the utmost seriousness").

76. *Worry About the Hackers You Don't Know*, CNN MONEY (last visited Feb. 5, 2013), http://money.cnn.com/video/technology/2011/07/26/t-tt-unknown-hackers.cnnmoney/ (referring to Anonymous as a renegade hacker group).

77. *Id*.

78. Zeljka Zorz, *The Escalating Cost of US Cybersecurity Plans*, (IN)SECURE (Feb. 15, 2012), http://www.net-security.org/secworld.php?id=12411 (explaining that the 2013 budget allocated $769 million to the Department of Homeland Security alone for cybersecurity initiatives and that the U.S. government as a whole is expected to spend $10.5 billion per year by 2015).

79. *See* Brenner, *supra* note 10, ¶ 56 ("[C]ybercrime is often transnational crime, which raises the issue of jurisdiction to prosecute the offender. Countries must examine their procedural law and, if necessary, amend it so they can legitimately exercise jurisdiction over cybercrimes.").

80. There have been incidents of foreign militaries or intelligence agencies targeting foreign governments. *See* KREKEL, *supra* note 14, at 72 (citing Chinese hackers targeting German government entities). These offenses may be subject to Article 104 despite being from a military entity. *See* MCM, *supra* note 11, pt. 4, at 41 (denouncing "offenses by all persons whether or not otherwise subject to military law").

81. *See* William Young, *A Check on Faint-Hearted Presidents: Letters of Marque and Reprisal*, 66 WASH & LEE L. REV. 895, 910 n.97 (2009) ("The area of cyber warfare is one of the few areas in which private individuals might still be more effective than the government in certain cases—especially in disrupting enemy communications and funding.").

82. *Id.* at 938 n.245.

83. *See* MCM, *supra* note 11, pt. 4, at 41–42 (explaining the scope of Article 104).

whether the group is a "hostile body."[84] Certainly, Al Qaeda and its associate forces are hostile to the United States.[85] As such, any cyberattacker communicating or otherwise assisting these obvious terrorist groups will be aiding a hostile body.

The issue gets slightly less obvious when considering agents of foreign governments. For example, China, Russia, and Venezuela are not hostile to the United States in the conventional sense.[86] But what happens if a domestic or foreign agent of one of these countries is captured for involvement in a cyberattack against the United States? DoD policy equates significant cyberattacks to hostile acts.[87] This policy shift in part deviates from traditional congressional views that covert actions are not typical military activities.[88]

Therefore, at least on some level, the United States can consider a government engaged in significant cyberattacks as a hostile body for the purposes of military justice.[89] Certainly, the international community appears inclined to view cyberwarfare as something less than "armed attack" under the laws of war.[90] But, again, Article 104 is a U.S. domestic law.[91] Moreover, nations facing cyberattacks are permitted to respond.[92] The types of

---

84. *See id.* The explanation in Article 104 refers to a discussion of "enemy" within Article 99, which defines the "enemy," in part, as "any hostile body that our forces may be opposing, such as a rebellious mob or band of renegades, and includes civilians as well as members of military organizations." *Id.* pt. 4, at 34.

85. Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARV. NAT'L SEC. J. 629, 647 (2011) ("The server might be a valid military target because it's being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations).").

86. An example of a purported Chinese cyberattack is as follows:

> For about 18 minutes on April 8, 2010, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, routing all traffic to about 15 percent of the Internet's destinations through servers located in China. This incident affected traffic to and from U.S. government (''.gov'') and military (''.mil'') sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others. Certain commercial websites were also affected, such as those for Dell, Yahoo!, Microsoft, and IBM.

U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 2010 REPORT TO CONGRESS 244 (2010), *available at* http://origin.www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf.

87. *See* Lynn, *supra* note 1 ("Just as the military defends against hostile acts from land, air, and sea, it must also be prepared to respond to hostile acts in cyberspace. Accordingly, the United States reserves the right, under the law of armed conflict, to respond to serious cyberattacks with an appropriate, proportional, and justified military response.").

88. Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEO. WASH. L. REV. 1162, 1171 n.53 (2011) (noting that traditional military activities are excluded from the scope of covert actions (citing 50 U.S.C. § 413b(e)(2) (2006)).

89. *See* Lynn, *supra* note 1 (discussing international perspectives on cyberwarfare).

90. *See* Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. 11, 11–12 (2011) (noting that cyberhostilities falling below the "armed attack" threshold are increasingly prevalent on the international stage).

91. U.C.M.J. art. 104 (2010) (to be codified at 10 U.S.C. § 904), *reprinted in* MCM, *supra* note 11, pt. 4, at 41–42.

92. *See* Lt. Cdr. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MIL. L. REV. 1, 27 (2009) ("The analysis of whether states can respond to cyberattacks with active defenses predominantly falls under *jus ad bellum*, which provides (1) the thresholds that cyberattacks must cross to be considered a use of force, which would then bring cyberattacks under the *jus in bello*, and (2) the legal options

cyberattacks that could elicit an internationally-sanctioned military response likely pertain to cyberattacks that transcend into the physical world.[93]

A military justice approach is merely one avenue that the United States can take. Indeed, many are increasingly arguing that cyberattacks against a nation can be considered to have emanated from hostile activity, particularly due to the threat of escalation from cyberwarfare to traditional armed conflict.[94] Importantly, a state of hostilities has historically existed prior to declared wars or military authorizations.[95] Courts have recognized that hostilities and/or armed conflict as applied to U.S. law do not begin when declarations or resolutions such as the Authorization for Use of Military Force (AUMF) are approved.[96] Therefore, a courts-martial panel or military judge could reasonably assert the possibility that intense cyberattacks and defenses constitute the existence of hostilities prior to conventional armed conflict.[97] Such an assertion relating to a hostile body can apply to agents of foreign powers. It also can apply to individuals associated with groups whose mission involves extensive cyberattacks against the United States.

D. Article 104's "Shadow Element" of Allegiance

For purposes of Article 104, a cyberenemy is any individual who, directly or indirectly, knowingly assists an organized enemy group with the group's mission toward attacking U.S. electronic infrastructure.[98] But it is worth noting that since 1950, courts-martial have never been used to prosecute non-servicemembers under Article 104,[99] although aiding the enemy has been

---

that states have to respond to cyberattacks.").

93. *See id.* ("[C]yberattacks provide terrorists a way to increase the destructive impact of physical attacks."); *see also* Michael N. Schmitt, "*Direct Participation in Hostilities" and 21st Century Armed Conflict*, *in* CRISIS MANAGEMENT AND HUMANITARIAN PROTECTION: FESTSCHRIFT FÜR DIETER FLECK 505, 526 (Horst Fischer et al. eds., 2004) ("[H]umanitarian law norms apply whenever computer network attacks attributable to a State are more than merely sporadic and isolated incidents and are either intended to cause injury, death, damage, or destruction (and analogous effects), or such consequences are foreseeable. This is so even if the attacks are unrelated to the classic use of military force.").

94. *See, e.g.*, Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 980 n.37 (2011) ("While financial crimes, the theft of IP, and extortion may be tolerated, cyber attacks against the host State or other nations that threaten to escalate hostilities are not.").

95. *See* United States v. Anderson, 38 C.M.R. 386, 389–92 (C.M.A. 1968) (Kilday, J., concurring) (citing conflicts ranging from the undeclared naval war with France in 1798 to Vietnam where hostilities and armed conflict existed prior to official resolutions, declarations, or authorizations).

96. N.Y. Life Ins. Co. v. Bennion, 158 F.2d 260, 264 (10th Cir. 1946) ("[T]he formal declaration by the Congress on December 8th was not an essential prerequisite to a political determination of the existence of a state of war commencing with the attack on Pearl Harbor.").

97. *See, e.g.*, *id.*

98. U.C.M.J. art. 104 (2010) (to be codified at 10 U.S.C. § 904), *reprinted in* MCM, *supra* note 11, pt. 4, at 41–42.

99. Convictions under Article 104 have typically been applied to U.S. prisoners of war who accepted some sort of parole from the enemy during the servicemember's detention. *See, e.g.*, United States v. Olson, 22 C.M.R. 250, 253 (C.M.A. 1957) (holding that a servicemember giving speeches that aid the enemy while a prisoner of war is a violation of Article 104); United States v. Batchelor, 22 C.M.R. 144, 151 (C.M.A. 1956) (holding that attempting to persuade others that the enemy was in the right violated Article 104); United States v. Dickenson, 20 C.M.R. 154, 163 (C.M.A. 1955) (holding that communicating with the enemy while a prisoner of war violated Article 104); *see also* United States v. Anderson, 68 M.J. 378, 387 (C.A.A.F. 2010) (sentencing soldier to life after emailing troop movements, military vehicle vulnerabilities, and other

charged against aliens prosecuted in military commissions.[100] Some contend that the aiding of enemy offense includes an allegiance requirement, although there is typically little to no analysis into the actual text of Article 104 and 106.[101] An allegiance or duty requirement would conceivably limit the scope of Article 104 to individuals with significant ties to the U.S., particularly citizens and lawful permanent residents.[102]

However, the text of Article 104 does not include any mention of an allegiance requirement.[103] In fact, the drafters of the MCM appeared to go out of their way to specifically apply Article 104 to any person, regardless of whether or not the individual was otherwise subject to military law.[104] In addition, Congress listed Article 104, along with the offense of spying, as the only offenses under the UCMJ to apply to both courts-martial and military commissions.[105] Such a legislative directive is important because military commissions typically cannot apply to U.S. citizens.[106]

A 2011 article in the Air Force Law Review referred to the incorrect assertions of the purported allegiance requirement of Article 104 as a "shadow element."[107] The genesis of the "shadow element" is based on confusion with

---

information to groups he thought were the enemy).

100. *See* Vijay M. Padmanabhan, *Norm Internalization Through Trials for Violations of International Law: Four Conditions for Success and Their Application to Trials of Detainees at Guantanamo Bay*, 31 U. PA. J. INT'L L. 427, 466 n.153 (2009) (stating that David Hicks and Omar Khadr were charged with, among other offenses, aiding the enemy based on their involvement in firefights between the Taliban and the U.S. military in the course of the war in Afghanistan); *see also Ex parte* Quirin, 317 U.S. 1, 20 (1942) (relating to Nazi saboteurs who were captured and tried via military commission after sneaking into the United States); Motion to Dismiss Charge 3 for Failure to State an Offense, United States v. Hicks, No. 04-001, at n.1 (C.M.C.R. Oct. 4, 2004) ("The American offense of 'aiding the enemy' has its origins in Articles 27 and 28 of the Articles of War of 1775, predating the American crime of treason . . . ."), *available at* http://www.defense.gov/news/Oct2005/d20051006vol9.pdf. The specific charge in *Quirin*, listed at the time as a violation of Article 81 of the Articles of War, matches the elements for the current UCMJ Article 104. *Quirin*, 317 U.S. at 1.

101. *See generally* David Glazier, *A Self-Inflicted Wound: A Half-Dozen Years of Turmoil Over the Guantanamo Military Commissions*, 12 LEWIS & CLARK L. REV. 131 (2008). In his critique of the military commissions system, Glazier argues that in order to commit the crime of aiding the enemy, one must "logically be a citizen or resident of the United States, or a resident of territory occupied by U.S. military forces who owes a temporary duty of allegiance to the occupier in exchange for its protection." *Id.* at 154. Glazier also attaches an allegiance requirement to Article 104. *Id*. The *Hamdan* court also briefly stated that, generally, a duty of loyalty exists. Hamdan v. United States, 696 F.3d 1238, 1245 n.4 (D.C. Cir. 2012). However, these statements are made in dicta, appear to be afterthoughts, and do not include any tangible analysis into the statutes and executive orders of Article 104 and 106, and indeed run contrary to the language of the UCMJ and executive orders. *Id.*

102. Glazier, *supra* note 101, at 154 ("[C]ommentators implicitly recognize that an individual must have a duty not to aid the enemy in order to be prosecuted . . . .").

103. U.C.M.J. art. 104 (2010) (to be codified at 10 U.S.C. § 904), *reprinted in* MCM, *supra* note 11, pt. 4, at 41–42.

104. MCM, *supra* note 11, pt. 4, at 41–42; *see also* United States v. Hamdan, 801 F. Supp. 2d 1247, 1294 (C.M. Comm'n R. 2011), *rev'd*, 696 F.3d 1238 (D.C. Cir. 2012) (observing that the Court of Military Commission Review noted in dicta that the absence of a breach of duty or allegiance is not in the elements and forms specifications, so the members are free to find enemy aliens with no such duty guilty of aiding the enemy).

105. Military Commissions Act of 2009, Pub. L. No. 111-84 §§ 1802, 123 Stat. 2574, 2611 (2009) (to be codified at 10 U.S.C. § 950(t)). Similarly, Articles 104 and 106 are the only punitive offenses under the UCMJ that Congress has approved for use under the Military Commissions Act of 2009.

106. *See Ex parte* Milligan, 71 U.S. (4 Wall.) 2, 121 (1866) (explaining that military commissions cannot be convened against U.S. citizens where civilian courts are functioning).

107. *See* Michael J. Lebowitz, *A Question of Allegiance: Choosing Between Dueling Versions of "Aiding the Enemy" During War Crimes Prosecution*, 67 A.F. L. REV. 131, 136–38 (2011) [hereinafter Lebowitz,

historic treason statutes that include allegiance requirements.[108] However, those who believe that Article 104 has an allegiance requirement overlook two important items. First, the historic aiding the enemy offense seemingly split off from the treason offense.[109] The intent of splitting aiding the enemy from treason appears to be solely based on the need for a military justice component to the elements of the offense.[110]

English jurisprudence, for example, as early as 1691 viewed aiding the enemy as a separate offense and consequently different from treason.[111] The second important item is the fact that, again, Article 104 and the MCM do not include an allegiance requirement as an element to the offense.[112] The statutory language only states that the offense applies to all persons whether or not otherwise subject to military law.[113]

E. Procedural Rights

1. Warnings

Without an allegiance requirement, the language associated with Article 104 through the UCMJ and MCM applies jurisdiction for trial by court-martial to anybody, including non-U.S. citizens, who otherwise meet the elements of the aiding the enemy offense.[114] If a suspected cyberenemy is captured by U.S. government officials, the individual could be transferred into military custody if such a policy was implemented.

The system for courts-martial is designed to provide rights geared toward servicemembers. As such, the alleged cyberenemy would invariably enjoy

---

Dueling Versions] (describing a "peculiar" additional element to the offense that "wormed its way into the legal discourse" without actually being written into the statute or historically accurate).

108. *Id*. at 137.

109. *See* Charles Warren, *What Is Giving Aid and Comfort to the Enemy*, 27 YALE L.J. 331, 332 (1918) (arguing that the early development of the law hints at the historic split between aiding the enemy and treason as those with an allegiance are guilty of treason, while others without a duty of allegiance conceivably are merely aiding the enemy); *see also* United States v. Olson, 22 C.M.R. 250, 256–57 (C.M.A. 1957) (noting an analogous line of cases involving the crime of treason that are distinguishable from aiding the enemy).

110. *See generally* Tara Lee, *American Courts-Martial for Enemy War Crimes*, 33 U. BALT. L. REV. 49 (2003). Lee notes:

> Congress authorized specific military jurisdiction over certain crimes unique to time of war—such as aiding the enemy and spying—as early as 1775. The original statutory Code of Articles of War, enacted in that year, provided at Article 27 that "[w]hosoever relieves the enemy with money, victuals, or ammunition, or knowingly harbors or protects an enemy . . ." and at Article 28 that "[w]hosoever holds correspondence with, or gives intelligence to, the enemy, either directly or indirectly . . ." shall each "suffer death, or such other punishment as a court-martial may direct."

Id. at 54 (quoting WILLIAM WINTHROP, MILITARY LAW AND PRECEDENTS 102 (2d ed. 1920)).

111. *See* Capt. Jabez W. Loane IV, *Treason and Aiding the Enemy*, 30 MIL. L. REV. 43, 59 (1965) (offering an extensive history of the parallel tracks between treason and aiding the enemy).

112. Glazier, *supra* note 101, at 176.

113. *See* U.C.M.J. art. 104 (2010) (to be codified at 10 U.S.C. § 904), *reprinted in* MCM, *supra* note 11, pt. 4, at 41–42 (using the words "any person").

114. *See* Lebowitz, *Dueling Versions*, *supra* note 107, at 149 ("Theoretically, when prosecuting alleged war criminals, military trial counsel could bypass a military commission altogether and instead take the accused straight to a court-martial. After all, Article 104 does assert jurisdiction over 'any person.'" (quoting U.C.M.J. art. 104)).

those same rights. This includes Article 31(b) warnings, which are recognized as going beyond the requirements of Miranda warnings in civilian practice.[115] From there, military trial counsel would draft a charge sheet listing the offenses under Article 104.

2. Capital Punishment

Conceivably, a cyberenemy can initiate an attack that transcends the electronic realm and into the physical world.[116] For example, electronic grids or water treatment facilities could be incapacitated or destroyed.[117] Deaths could result from these physical breakdowns. Because Article 104 is a capital offense, a cyberenemy under these circumstances could face the death penalty.[118]

However, the cyberenemy would not be charged with the offense of murder because that punitive article in the UCMJ generally only applies to servicemembers.[119] Instead, the charge sheet would be drafted in such a manner to reflect that the cyberenemy, pursuant to Article 104, knowingly aided an enemy group by using and providing computer skills, equipment, and malicious coding in implementing a cyberattack that led to the death.

3. Courts-Martial Process

Once charges are preferred, the process would commence just like a typical court-martial.[120] The accused would be detailed a military defense counsel, with the option for civilian defense counsel as well.[121] The accused cyberenemy would be afforded the right to an Article 32 hearing.[122] A

115. U.C.M.J. art. 31(b) (2010) (to be codified at 10 U.S.C. § 831(b)), *reprinted in* MCM, *supra* note 11, app. 2, at 9.

116. *See* Lynn, *supra* note 1 ("In a development of extraordinary importance, cyber technologies now exist that are capable of destroying critical networks, causing physical damage, or altering the performance of key systems."); *supra* note 17 and accompanying text (discussing the introduction of a Trojan Horse program into Soviet computer systems that caused a gas pipeline to explode in Trans-Siberia).

117. *See* WILSON, *supra* note 2, at 6 (discussing the views of experts who define cyberterrorism to include computer attacks that have non-cyber effects including power outages and water contamination).

118. U.C.M.J. art. 104.

119. *See* U.C.M.J. art. 118 (2010) (to be codified at 10 U.S.C. § 918), *reprinted in* MCM, *supra* note 11, pt. 4, at 62 (defining "murder" and asserting jurisdiction over "any person subject to this chapter"); *see also* U.C.M.J. art. 2 (2010) (to be codified at 10 U.S.C. § 802), *reprinted in* MCM, *supra* note 11, app. 2, at 1–2 (including servicemembers within UCMJ jurisdiction).

120. *See generally* U.C.M.J. art. 22 (2010) (to be codified at 10 U.S.C. § 822), *reprinted in* MCM, *supra* note 11, app. 2, at 7 (defining those authorized to convene courts-martial); U.C.M.J. art. 26(b) (2010) (to be codified at 10 U.S.C. § 826(b)), *reprinted in* MCM, *supra* note 11, app. 2, at 8 (providing qualifying criteria for military judge); U.C.M.J. art. 51 (2010) (to be codified at 10 U.S.C. § 851), *reprinted in* MCM, *supra* note 11, app. 2, at 15 (establishing voting and ruling procedures for courts-martial); Robinson O. Everett, *The Law of War: Military Tribunals and the War on Terrorism*, 48 FED. LAW. 20, 20–21 (2001) (summarizing the typical court-martial process); Gordon Forester Jr. & Kevin J. Barry, *Military Commissions: Meeting American Standards of Justice*, 49 FED. LAW. 28, 30 (2002) (explaining the difference between military commissions and courts-martial).

121. U.C.M.J. art. 838(b)(1)–(2) (2010) (to be codified at 10 U.S.C. §§ 838(b)(1)–(2)), *reprinted in* MCM, *supra* note 11, app. 2, at 11.

122. U.C.M.J. art. 32(b) (2010) (to be codified at 10 U.S.C. § 832(b)), *reprinted in* MCM, *supra* note 11, app. 2, at 9–10.

convening authority will review the charges and ultimately determine whether or not to refer the case to a general court-martial.[123] The convening authority in a cyberenemy case would likely be the general officer that commands the overall unit responsible for the cyberenemy's confinement.[124]

IV. MILITARY COMMISSION

A. Capability in Handling International Cyberenemies

Although the MCM seemingly authorizes the limited option of prosecuting non-U.S. citizens pursuant to Articles 104 and 106, Congress also approved the use of military commissions for aiding the enemy offenses.[125] Historically, military commissions have been used to prosecute war crimes perpetrated by foreign individuals involved in hostilities against the United States.[126] Article 104 specifically provides jurisdiction for military commissions against alien personnel accused of aiding the enemy.[127] This provision is relatively unique because aiding the enemy is not considered a violation of the law of war.[128]

But in the case of cyberenemies, military commissions could be superior forums for prosecution over courts-martial and federal courts.[129] The reason is because modern military commissions were created after September 11, 2001, to compensate for the fact that law enforcement personnel were not always the ones involved in capturing detainees or obtaining evidence.[130] Instead, military personnel, intelligence agencies, and foreign governments were sometimes engaged in such endeavors under wartime and exigent

123. *See generally* U.C.M.J. art. 22 (2010) (to be codified at 10 U.S.C. § 822), *reprinted in* MCM, *supra* note 11, app. 2, at 7 (listing those officials with the authority to convene general courts-martial).

124. *See* Lebowitz, *Dueling Versions*, *supra* note 107, at 150 (stating that a theoretical court-martial relating to Guantanamo Bay detainees charged with offenses pursuant to Article 104 would be subject to the commander of Joint Task Force Guantanamo); *see also* U.C.M.J. art. 22(a)(6) (authorizing "the commander in chief of a fleet; the commanding officer of a naval station or larger shore activity of the Navy beyond the United States" to convene a general court-martial).

125. Military Commissions Act of 2009, Pub. L. No. 111-84, § 1802, 123 Stat. 2574, 2574–612 (2009) (to be codified at 10 U.S.C. §§ 948–50) ("A military commission under this chapter shall have jurisdiction to try persons subject to this chapter for any offense made punishable by this chapter, sections 904 . . . ."). Aiding the enemy is a section 904, i.e., Article 104, offense.

126. *See, e.g.*, *id.*; *see also* Robert M. Gates, *Foreword* to MANUAL FOR MILITARY COMMISSIONS: UNITED STATES (2010) [hereinafter MMC] (applying the procedures and rules from courts-martial unless otherwise noted or "where required by the unique circumstances of the conduct of military and intelligence operations during hostilities or by other practical need"); *Military Commissions History*, MILITARY COMMISSIONS, http://www.mc.mil/ABOUTUS/ MilitaryCommissionsHistory.aspx (last visited Feb. 5, 2013) (detailing the United States' historic use of military commissions from 1778 to 2012).

127. U.C.M.J. art. 104 (2010) (to be codified at 10 U.S.C. § 904), *reprinted in* MCM, *supra* note 11, pt. 4, at 41–42.

128. *See id.* (making no reference to the law of war).

129. *See, e.g.*, Harvey Rishikof, *Is it Time for a Federal Terrorist Court? Terrorists and Prosecutions: Problems, Paradigms, and Paradoxes*, 8 SUFFOLK J. TRIAL & APP. ADVOC. 1, 10 (2003) (discussing the use of military commissions against suspected terrorists).

130. *Id.*; *see also* Michael J. Lebowitz, *The Value of Claiming Torture: An Analysis of Al-Qaeda's Tactical Lawfare Strategy and Efforts to Fight Back*, 43 CASE W. RES. J. INT'L L. 357, 376 (2010) [hereinafter Lebowtiz, *Claiming Torture*] (explaining how military commissions formed in response to the 9/11 attacks).

circumstances.[131] Although competent to handle complex cases, courts-martial may not be the most practical forum when national security concerns become paramount. For example, when tracing a cyberattack, cyberforensics can lead investigators through multiple countries, involving numerous diplomatic sensitivities.[132] Without proper assurances, the trial and discovery process could potentially risk exposing confidential informants, as well as top secret offensive, defensive, and investigative methods pertaining to cyberactivity.[133] Again, cyberforensics is an extremely complex art that often goes well beyond traditional investigating techniques. The most vulnerable portion of government and economic national security functions are tied to electronic systems.[134] As a result, the government must balance its interest in prosecuting cyberenemies with its need to protect sensitive national security priorities.[135] Convening a military commission and using Article 104 as its punitive offense is one way in maintaining this balance.

If the United States opts to prosecute certain cyberenemies via military commission, it must first ensure that these proceedings are legally sufficient. By using Article 104 as the primary offense, the government will avoid virtually all *ex post facto* issues because Article 104 has applied to military commissions since 1950.[136] Legislation authorizing military commissions in cyberenemy cases should likely be modeled after the Military Commissions Act of 2009 (MCA 2009) in terms of procedural and evidentiary rights. In fact, cyberenemy cases involving Al Qaeda, the Taliban, or associated forces likely can be prosecuted in a military commission pursuant to the MCA 2009.[137]

B. Prosecuting Foreign Cyberattackers

1. Jurisdiction

The MCA 2009 can also likely be used against certain classes of

131. *See* Lebowitz, *Claiming Torture*, *supra* note 130, at 376 (describing the benefits of military commissions for intelligence agencies).

132. *See* Rishikof, *supra* note 129, at 34 (advocating for a specialized court, as a matter of public policy, to serve as the center of expertise on terrorist networks in order to generate confidence and credibility with the world community).

133. *See, e.g.*, Williams, *supra* note 88, at 1182–91 (exploring why cyberspace is "a unique medium for the conduct of espionage and covert action").

134. *Id.*

135. *See* Lebowitz, *Claiming Torture*, *supra* note 130, at 376 ("Agencies such as the CIA and NSA are historically intelligence-gathering organizations, as opposed to law enforcement groups such as the FBI and the Criminal Investigation Task Force (CITF). As a result, the military commission process allows the CIA to focus on national security while not voiding the prospects of seeking a conviction in either federal court or via military commission.").

136. *See* Note, *Military Jurisdiction Over Discharged Servicemen: Constitutionality and Judicial Protection*, 67 HARV. L. REV. 479, 479 n.1 (1954) (explaining that the Uniform Code of Military Justice was enacted in 1950).

137. Military Commissions Act of 2009, Pub. L. No. 111-84, § 1802, 123 Stat. 2574, 2574–76 (2009) (to be codified at 10 U.S.C. § 948(a)(7)(C)); *see also* Act of Sep. 18, 2001, Pub. L. No. 107-40, 115 Stat. 224 (2001) (authorizing use of Military Force against al-Qaeda, the Taliban, and associated forces).

cyberattackers who are not affiliated with Al Qaeda or the Taliban.[138] Jurisdiction under the MCA 2009 rests with the enemy operative being an "unprivileged enemy belligerent."[139] This is defined as an individual who: "(a) has engaged in hostilities against the United States or its coalition partners; (b) has purposefully and materially supported hostilities against the United States or its coalition partners; or (c) was part of Al Qaeda at the time of the alleged offense."[140] Therefore, even if the cyberattacker was not affiliated with Al Qaeda, a military commission would have jurisdiction over certain classes of alien cyberenemies engaged in or supporting hostilities against the United States or its partners.[141]

2. Pertinent Offenses Triable by Military Commission

Under this scenario, a military commission convened pursuant to the MCA 2009 would not be limited to Article 104 offenses.[142] Any number of the offenses triable by the MCA 2009 would apply to cyberattackers operating as part of a hostile force against the United States.[143] Such a prosecution within the MCA 2009 would effectively treat this class of cyberattacks as war crimes.[144]

For example, a significant cyberattack upon civilian infrastructure could equate to the offenses of attacking civilian objects and destruction of property in violation of the law of war.[145] In addition, a cyberattack against a target such as a water-treatment facility also could equate to attacking civilians, particularly if the attack manifests into a physical event upon the population.[146] A cyberattack on a hospital could be construed as attacking protected property.[147] The MCA 2009 also provides jurisdiction for murder in violation of the law of war if a cyberattacker deliberately causes a death—for example, if the cyberattacker infects the power or traffic grids.[148] Similarly, the Manual

138. Military Commissions Act of 2009 § 1802, 123 Stat. at 2574–81 (to be codified at 10 U.S.C. §§ 948(a)(7), (c)–(d)).

139. *Id.* § 1802, 123 Stat. at 2576 (to be codified at 10 U.S.C. § 948(c)–(d)).

140. *Id.* § 1802, 123 Stat. at 2575 (to be codified at 10 U.S.C. § 948(a)(7)).

141. *Id.* § 1802, 123 Stat. at 2575 (to be codified at 10 U.S.C. § 948(d)).

142. *Id.* ("A military commission under this chapter shall have jurisdiction to try persons subject to this chapter for any offense made punishable by this chapter, sections 904 and 906 of this title (articles 104 and 106 of the Uniform Code of Military Justice), or the law of war, whether such offense was committed before, on, or after September 11, 2001, and may, under such limitations as the President may prescribe, adjudge any punishment not forbidden by this chapter, including the penalty of death when specifically authorized under this chapter. A military commission is a competent tribunal to make a finding sufficient for jurisdiction.").

143. *See infra*, notes 144–58 and accompanying text (discussing offenses triable by the MCA 2009).

144. *See generally*, Military Commissions Act of 2009 § 1802, 123 Stat. at 2190 (pertaining to offenses committed in violation of the law of war).

145. *Id.* § 1802, 123 Stat. at 2607 (to be codified at 10 U.S.C. §§ 950(t)(3), (t)(16)); MMC, *supra* note 126, pt. 4, at 4, 13–14.

146. Military Commissions Act of 2009 § 1802, 123 Stat. at 2607 (to be codified at 10 U.S.C. § 950(t)(2)); MMC, *supra* note 126, pt. 4, at 3–4.

147. Military Commissions Act of 2009 § 1802, 123 Stat. at 2607 (to be codified at 10 U.S.C. § 950(t)(4)); MMC, *supra* note 126, pt. 4, at 5.

148. *See* Military Commissions Act of 2009 § 1802, 123 Stat. at 2607 (to be codified at 10 U.S.C. § 950(t)(15)) (explaining murder in violation of the law of war); MMC, *supra* note 126, pt. 4, at 13 (establishing the elements of murder).

for Military Commissions (MMC) regards terrorism as a war crime.[149] As such, a successful cyberattacker could be prosecuted for terrorism if the elements are established.[150]

Moreover, either a successful or unsuccessful cyberattacker could be subject to the offense of providing material support for terrorism so long as the offense occurred after 2006.[151] The material support offense generally applies to those who knowingly assist in the preparation or carrying out of an act of terrorism under the context of hostilities.[152] "Material support or resources" includes assisting with any tangible or intangible service, including those related to communications equipment.[153] As such, an individual knowingly assisting a hostile organization through a cyberattack falls into the material support punitive offense, so long as the planned cyberattack qualifies as an act of terrorism.[154]

C. Cyberattacks Within the Context of Hostilities

The elements of these offenses do not specifically mention cyberattacks.[155] However, nothing within the MCA 2009 or the MMC limits such charges to conventional attacks.[156] A key element in prosecuting significant cyberenemies through the MCA 2009 is whether or not the attack took place "in the context of and [was] associated with hostilities."[157] With regard to cyberattackers, there must be some demonstrable evidence reflecting that the cyberattack took place under the guise of hostilities between the cyberenemy's organization and the United States.[158]

To prove this element, the onus is on the military jury, also referred to as military commission panel members, to properly consider and find beyond a reasonable doubt that an armed conflict existed between the United States and

149. Military Commissions Act of 2009 § 1802, 123 Stat. at 2610 (to be codified at 10 U.S.C. § 950(t)(24)); MMC, *supra* note 126, pt. 4, at 19.

150. Elements of terrorism under the MMC are "(1) intentionally kill[ing] or inflict[ing] great bodily harm on one or more protected persons or engag[ing] in an act that evinced a wanton disregard for human life; (2) . . . in a manner calculated to influence or affect the conduct of government or civilian population by intimidation, coercion, or to retaliate against government conduct; and (3) [t]he killing, harm or wanton disregard for human life took place in the context of and was associated with hostilities." MMC, *supra* note 126, pt. 4, at 19.

151. Military Commissions Act of 2009 § 1802, 123 Stat. at 2610–11 (to be codified at 10 U.S.C. § 950(t)(25)); MMC, *supra* note 126, pt. 4, at 20. Material Support for Terrorism and Conspiracy offenses are only viable charges as war crimes if the acts occurred after 2006. In *Hamdan*, the D.C. Circuit held that charging defendants for war crimes under the material support offense for acts prior to 2006 was a violation of the ex post facto clause. Hamdan v. United States, 696 F.3d 1238, 1241 (D.C. Cir. 2012).

152. Military Commissions Act of 2009 § 1802, 123 Stat. at 2610–11 (to be codified at 10 U.S.C. § 950(t)(25)); MMC, *supra* note 126, pt. 4, at 20.

153. MMC, *supra* note 126, pt. 4, at 20.

154. *Id.*

155. *See generally id.* pt. 4 (stating the elements of these crimes without addressing cyberattacks in particular).

156. *See* Military Commissions Act of 2009 § 1802, 123 Stat. at 2575–76 (to be codified at 10 U.S.C. §§ 948(b), (d)) (authorizing military commissions and establishing their jurisdiction, without limiting them to conventional attacks).

157. *Id.* § 1802, 123 Stat. at 2576 (to be codified at 10 U.S.C. § 948(d)).

158. *Id.* § 1802, 123 Stat. at 2606–07 (to be codified at 10 U.S.C. §§ 950(p)–(q)).

the cyberenemy organization.[159] The Court of Military Commissions Review (CMCR), for example, recognized that video evidence prepared by an expert effectively proved that a state of hostilities existed.[160]

Taken together, it is the military commission panel members' responsibility to consider the issue of whether or not hostilities existed as one of the elements of each charge of the MCA 2009. Therefore, it is conceivable that evidence can be presented at trial reflecting upon the extent of the attacks, counterattacks, and attempted cyberattacks initiated by both sides of the cyberconflict, as well as the significant cyberdefenses employed by the United States and perhaps the opposing side.[161]

Panel members are tasked with the responsibility of considering, for example: 1) whether an armed conflict existed between the United States and the opposing force at the time of the offense; 2) the length, duration, and intensity of hostilities between the parties; 3) whether there was protracted armed violence between governmental authorities and organized armed groups; 4) whether and when the United States decided to employ the combat capabilities of its armed forces to meet the organized enemy threat; 5) the number of persons killed or wounded on each side; 6) the amount of property damage on each side; 7) statements of the leaders of both sides indicating their perceptions regarding the existence of an armed conflict, including the presence or absence of a declaration to that effect; and 8) any other facts or circumstances the panel members may deem relevant to determining the existence of armed conflict.[162] In *Hamdan*, the panel members were not

159. *See, e.g.*, United States v. Hamdan, 801 F. Supp. 2d 1247, 1278 n.54 (C.M. Comm'n R. 2011), *rev'd*, 696 F.3d 1238 (D.C. Cir. 2012) (explaining the requirement to find beyond a reasonable doubt that a conflict exists between the United States and a terrorist organization).

160. *Id.* at 1255 n.5.

161. The court held that the military judge's instructions to panel members met the standard for a reasonable doubt determination regarding the hostilities element of the charged offenses. *Id.* at 1278 n.54. The pertinent portion of the military judge's instructions on this element is as follows:

> [T]he government must prove beyond a reasonable doubt that the actions of the accused took place in the context of and that they were associated with armed conflict. In determining whether an armed conflict existed between the United States and al Qaeda and when it began, you should consider the length, duration, and intensity of hostilities between the parties, whether there was protracted armed violence between governmental authorities and organized armed groups, whether and when the United States decided to employ the combat capabilities of its armed forces to meet the al Qaeda threat, the number of persons killed or wounded on each side, the amount of property damage on each side, statements of the leaders of both sides indicating their perceptions regarding the existence of an armed conflict, including the presence or absence of a declaration to that effect, and any other facts or circumstances you consider relevant to determining the existence of armed conflict. The parties may argue the existence of other facts and circumstances from which you might reach your determination regarding this issue. In determining whether the acts of the accused took place in the context of and were associated with an armed conflict, you should consider whether the acts of the accused occurred during the period of an armed conflict as defined above, whether they were performed while the accused acted on behalf of or under the authority of a party to the armed conflict, and whether they constituted or were closely and substantially related to hostilities occurring during the armed conflict and other facts and circumstances you consider relevant to this issue. Counsel may address this matter during their closing arguments, and may suggest other factors for your consideration. Conduct of the accused that occurs at a distance from the area of conflict can still be in the context of and associated with armed conflict, as long as it was closely and substantially related to the hostilities that comprised the conflict.

Id.

162. *Id*.

required to find that each individual plank of the instruction was applicable to proving the hostilities element. Instead, the members only needed to *consider* each plank in making their overall decision.[163]

Due to the relatively clandestine nature of cyberwarfare, there has yet to be a declared state of hostilities or outright war. This should not, however, restrict the use of the MCA 2009 in cases involving cybercampaigns against the United States. As mentioned above, courts have historically concluded that a state of hostilities existed prior to declared wars or military authorizations.[164] Courts have recognized that hostilities and/or armed conflict as applied to United States law do not begin when declarations or resolutions such as the Authorization for Use of Military Force (AUMF) are approved.[165] Applied to the issue of cyberenemies, one can assert the possibility that hostilities existed prior to any specific authorization similar to the AUMF.[166] The proper fact finder for the ultimate determination in the event of a military commission against an accused cyberattacker, again, is the panel members pursuant to the CMCR precedent.

D. Expanding Scope of Military Commissions

The modern military commissions were born from the war against Al Qaeda.[167] It is conceivable that an additional authorization for military commissions specifically relating to cyberenemies could be crafted. By authorizing cyberenemy-specific military commissions, a potentially broader-based jurisdiction will be available.[168] In this manner, non-U.S. citizens caught aiding cyberattackers within foreign governments to cyberterrorist groups can be subject to trial by military commission.

As an aside, it should be noted that the various incarnations of the military commissions system created since September 11, 2001, provided for an offense called "wrongfully aiding the enemy."[169] That offense, codified by

163. *Id.* In listing the individual planks to determine whether an armed conflict existed and when it began, the trial judge instructed the panel members that they should "consider" each plank, as well as "any other fact or circumstances you consider relevant to determining the existence of an armed conflict." *Id.* As such, the trial judge effectively provided a detailed list of planks for the panel members to consider, but did not require that each specific plank be satisfied as a basis for their determination.

164. *See* United States v. Anderson, 38 C.M.R. 386, 389–92 (C.M.A. 1968) (Kilday, J., concurring) (citing conflicts ranging from the undeclared naval war with France in 1798 to Vietnam where hostilities and armed conflict existed prior to official resolutions, declarations, or authorizations).

165. New York Life Ins. Co. v. Bennion, 158 F.2d 260, 264 (10th Cir. 1946) ("[T]he formal declaration by the Congress on [8 December 1941] was not an essential prerequisite to a political determination of the existence of a state of war commencing with the attack on Pearl Harbor.").

166. *See generally* Authorization for the Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001) (stating that recent attacks launched against the United States form one basis underlying the authorization of military force against Al Qaeda, the Taliban, and associated forces).

167. *Id.*; *see also* Military Commissions Act of 2009, Pub. L. No. 111-84 § 1802, 123 Stat. 2574, 2574 (2009) (to be codified at 10 U.S.C. § 948(a)(7)(c)) (defining an "unprivileged enemy belligerent" as an individual who was a part of Al Qaeda).

168. *See* Military Commissions Act of 2009, § 1802, 123 Stat. at 2574 (to be codified at 10 U.S.C. § 948(a)(7)(c)) (defining unprivileged enemy belligerents in a way that does not include cyberenemies).

169. Military Commissions Act of 2009 § 1802, 123 Stat. at 2607 (to be codified at 10 U.S.C. § 950(t)) (including "wrongfully aiding the enemy" within the scope of crimes triable by military commission); *see also* MMC, *supra* note 126, pt. 4, at 20–21 (discussing the crime of wrongfully aiding the enemy).

Congress in the MCA 2009, created an allegiance requirement.[170] However, in that same piece of legislation, Congress also specifically stated that the military commission had jurisdiction over Article 104 as well.[171] When approving this legislation, Congress did not amend Article 104.[172] As a result of both items being directly addressed within the same piece of legislation, the 2011 Air Force Law Review article on the subject argued that prosecutors were provided a choice of law between wrongfully aiding the enemy within the MCA 2009 and aiding the enemy within Article 104.[173] However, with respect to Article 104, the same arguments as laid out above with respect to courts-martial also apply to Article 104 within a military commission against a cyberenemy.

V. CONCLUSION

As cyberforensics capabilities develop, the United States will at some point find itself in position to capture individuals involved in cyberattacks. Depending on the nature and severity of the cyberattack, U.S. officials may be forced to develop a policy determining whether to treat the accused cyberenemy as a common criminal or as someone engaged in war or hostilities against the United States. After September 11, 2001, the United States deemed individuals involved in certain acts of terrorism to fall under military justice as opposed to federal courts. Military commissions were authorized for some of those cases. Military commissions provide a wide range of punitive offenses that, if applied to cyberattackers, would effectively treat certain classes of significant cyberattacks as war crimes. Conversely, Article 104 and Article 106 provide an untested but potentially viable military justice option for certain acts of cyberattacks and cyberspying through traditional courts-martial.

170. MMC, *supra* note 126, pt. 4, at 20–21 (describing "wrongfully aiding the enemy" in part as "[a]ny person subject to this chapter who, in breach of an allegiance or duty to the United States, knowingly and intentionally aids an enemy of the United States, or one of the co-belligerents of the enemy").

171. Military Commissions Act of 2009 § 1802, 123 Stat. at 2574 (to be codified at 10 U.S.C. § 948). In the Military Commissions Act of 2006 (MCA 2006), Congress amended UCMJ Article 104 to not apply to military commissions subject to the MCA 2006. Military Commissions Act of 2006, Pub. L. No. 109-366 § 4, 120 Stat. 2600, 2631 (2006). However, the MCA 2009 specifically established jurisdiction for charging alien unprivileged enemy belligerents with UCMJ Article 104. Military Commissions Act of 2009 § 1802, 123 Stat. at 2574 (to be codified at 10 U.S.C. § 948(a)(7)).

172. Military Commissions Act of 2009 § 1802, 123 Stat. at 2574 (to be codified at 10 U.S.C. § 948).

173. Lebowitz, *Dueling Versions*, *supra* note 107, at 143.