An Ethical Decision-Making Tool for Offensive Cyberspace Operations

Maj Benjamin Ramsey, USAF, PhD

Although international cyberspace espionage has been around for decades, offensive cyberspace operations (OCO) designed to create wartime effects are relatively nascent. The USAF added cyberspace as a domain in which it would "fly, fight, and win" to its mission statement in 2005, but the development of a sizable military OCO force in the US did not begin in earnest until the establishment of US Cyber Command (USCYBERCOM) in 2010. Meanwhile, only a few international examples of successful OCO integration into military operations have yet been made public. For example, OCO suppressed Syrian air defenses during the 2007 Israeli air strikes and coordinated OCO bolstered the 2008 Russian invasion of Georgia.[1] As USCYBERCOM reaches full operational capability, it is imperative that it conduct OCO, not only in accordance with international law, but also in an ethically responsible manner.

The most comprehensive study to date on the applicability of international law to cyberspace conflict is the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, in which 19 legal experts under the direction of Professor Michael Schmitt derived 154 black-letter rules from existing law.[2] The legal experts reached a consensus on 108 of these rules, including some straightforward applications of the Law of Armed Conflict (LOAC) to civilian protections. Legal opinions were divided on the remaining 46 rules, 9 of which had significant aspects relevant to OCO but also eluded a majority opinion. This article recommends an ethical decision-making tool for OCO and uses those contentious nine legal rules from the *Tallinn Manual 2.0* as example cases to consider ethical and sustainable norms in cyberspace.

Ethical and Legal Norms for Offensive Cyberspace Operations

The first ethical analysis of OCO by a moral philosopher was by philosophy professor Dr. Randall Dipert in 2010.[3] In his work, Dipert articulated three of the most challenging aspects of OCO: operations can be nonattributable, defenses are expensive and failure-prone, and there are no rare or exotic components in OCO weapons

that could inhibit their proliferation. Dipert also argued that existing international law and Just War Theory do not straightforwardly apply to OCO. Militaries can dramatically weaken opponent forces using OCO without necessarily causing death or permanent property damage, and thus circumvent the *casus belli* of traditional Just War Theory. Most importantly, Dipert predicted a long period to come of "low-level, multilateral cyberwarfare, a Cyber Cold War, as a game-theoretic equilibrium is sought."[4]

Dr. Brian Mazanec, a defense and strategic studies professor, came to a similarly bleak conclusion in his rebuttal to optimism about international cooperation and order in cyberspace: "norm evolution theory for emerging-technology weapons leads one to conclude that constraining forms for cyberwarfare. . . may never successfully emerge."[5] The principal actors for OCO include the US, China, and Russia, none of which consider the emergence of constraining norms that would curtail sovereign options to be in their self-interest.[6]

Russia and the US appear to be trending toward a consensus that OCO: (1) should never deliberately harm civilians and civilian infrastructure, (2) should be directed at legitimate military targets with the aim of minimizing collateral damage, (3) are equivalent to kinetic attacks of equal harm, and (4) is constrained by the principle of economy of force.[7] Unsurprisingly, these rules also appear in the *Tallinn Manual 2.0* with substantial legal expert consensus.

Perhaps no legal area concerning OCO is more contested than that of *jus ad bellum* (right to war), or what OCO actions could trigger armed conflict. While China and the US have officially agreed to "pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace," a significant divide exists between the Chinese and US positions on OCO use of force.[8] For example, the Chinese position is a strict positivist reading of the United Nations (UN) Charter's prohibition on the use of force, and in March 2017 the first official Chinese cyber strategy called on all states to avoid cyberspace militarization.[9] Conversely, the US position is that the "inherent right of self-defense potentially applies against *any* illegal use of force" (emphasis added).[10] The perspective of the *Tallinn Manual 2.0* falls between the Chinese and US extremes concerning the use of force; the *Tallinn Manual 2.0* reflects the position in the 1986 International Court of Justice case of *Nicaragua v. United States* that there is a difference between "use of force" as used in Article 2(4) of the UN Charter and "armed attack" that justifies self-defense under Article 51.[11] China, thus, rejects the *Tallinn Manual 2.0* perspective as too permissive, and the US rejects the same perspective as too restrictive.

A compelling solution to the challenge of normalizing international OCO without imposing stipulations is to follow the successful example of how the 2009 *Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict* addressed private security companies.[12] The *Montreux Document* underscored best practices that developed from the failure of existing laws and regulations rather than assert policies and restrictions on state operations. Events such as the 2007 Nisour Square incident in Baghdad, when US military contractors killed 17 civilians while escorting an embassy convoy, fostered international resolve to clarify "what the role for [private military and security companies] in armed conflicts is and should be."[13] The first half of the *Montreux Document* outlined pertinent legal obligations, and the

second half outlined good practices for states to follow that were not legally binding. The *Montreux Document* stated early on that it was not the final word on the matter, but that this was also never the intention.[14] Cyberspace is a domain different from all others in that the US is no longer the single dominant state for force projection; the multipolar nature of power and influence in cyberspace means that norms can only emerge from the shared objectives of all principal actors involved.

Original Position and Ethical Offensive Cyberspace Operations

Moral and political philosopher John Rawls introduced the *original position* as a central feature of his landmark book, *A Theory of Justice*, in 1971.[15] In this book, Rawls described a thought experiment, in which parties select principles of the society they will live in, but behind a "veil of ignorance" as to their individual ethnicity, social status, gender, and lifestyle. The idea behind the original position is that parties are forced to select societal principals that will be rational and fair since the parties do not know their ultimate position in the society undergoing design. Rawls understood that human nature is essentially self-centered, so the determination of what is fair must be made without consideration of personal privilege.

In cyberspace, there is no singularly dominant state, and OCO is largely nonattributable. None of the principal actors, therefore, have a privileged role to play in formalizing international norms. The situation closely mirrors that of the original position described by Rawls; the future balance of power in cyberspace is unknowable. The US, China, and Russia should leverage original-position thought experiments to determine what guidelines for OCO would be considered fair and sustainable to the international community as a whole.

Nine Test Cases for Ethical Offensive Cyberspace Operations

This section examines nine of the rules applicable to cyberspace operations for which expert opinion was thoroughly divided based on current law. Using the principal of the original position as an ethical decision-making tool for responsible state behavior, this section proposes behaviors with respect to each rule that will contribute to a fair, sustainable, and responsible normalization of cyberspace.

Rule 4: Violation of Sovereignty

According to international law, a state must not conduct cyberspace operations that violate the sovereignty of another state. On this point, the international group of experts was divided on whether a cyberspace operation that "results in neither physical damage nor the loss of functionality" amounts to a violation under this rule.[16]

A widely underappreciated fact about OCO is that detailed intelligence collection of the cyberspace environment is a fundamental prerequisite to force projection in the domain. Intelligence collection in cyberspace, just like its predecessors—human intelligence, imagery intelligence, and signals intelligence operations—is instrumental to collective international security. Thus, all of the primary actors presently execute invasive, yet nonharmful intrusions, into adversary cyberspace to perform

reconnaissance, gather intelligence, and to prepare OCO options for senior leadership in the event of armed conflict. As Simon Chesterman, the dean and law professor at the National University of Singapore Faculty of Law, succinctly put it, the "collection of intelligence is more than tolerated, and may actually be encouraged."[17] The universality of intelligence collection operations into adversary cyberspace occur with tacit international acceptance, in part, because accurate intelligence can help mitigate collateral damage and political miscalculations. From the original position, such maneuvers in cyberspace are apparent as an ethical necessity of the domain.

Rule 9: Territorial Jurisdiction

A state may exercise territorial jurisdiction over cyberspace infrastructure and persons engaged in cyberspace activities on its territory; cyberspace activities originating in, or completed on, its territory; or cyberspace activities having a substantial effect in its territory.[18] Under this rule, the international group of experts could not determine whether a state may exercise jurisdiction over data that simply traverses its territory *en route* to the intended destination.

A point not specifically addressed within the discussion regarding Rule 9 is that sensitive data in transit is frequently encrypted and is almost certainly encrypted when in support of OCO. In any event, the states through which the associated data passes are both arbitrary and temporally dynamic as a result of network best-effort routing. The transited states are furthermore unaware of the specific content of encrypted messages passing through their territorial cyberspace infrastructure. Pragmatically, the opportunities and motivations of transited states to seek jurisdiction will be relatively rare, and thus can be ethically addressed on a case-by-case basis, in "a reasonable fashion and with due regard for the interests of other states," as proposed by the international group of experts.[19] From the original position, it is clear that the primary actors would not select to relinquish jurisdiction to other states based on arbitrary or constantly changing data traversal of state network infrastructure.

Rule 22: Limitations on Countermeasures

Countermeasures conducted in cyberspace, as in other domains, must not violate fundamental human rights, amount to belligerent reprisals, violate peremptory norms, or violate diplomatic or consular inviolability.[20] While the bulk of the limitations on countermeasures discussion is unambiguous, the international team of experts could not reach a consensus on the applicability of the right to privacy as a fundamental human right, and therefore a limit on legal countermeasures. The *Tallinn Manual 2.0* points out that "whether or how human rights apply extraterritorially is unsettled and controversial."[21]

Despite the efforts of privacy advocates globally, the principal actors in cyberspace currently do not interpret privacy rights as applying extraterritorially, with the exception of reciprocal protections codified by treaty. States such as China and Russia do not appear to value privacy as even fundamental human right of their own citizens. Any attempt by a state to unilaterally impose extraterritorial privacy rights on international cyberspace would be futile for the foreseeable future, a fact that is evident from the original position. The ethical and responsible norm is,

therefore, for a state to select the most effective countermeasures available, while fully respecting widely-accepted human rights and also respecting privacy rights to the extent obligated by treaty and domestic law.

Rule 34: Applicability

Simply stated, international human rights law applies to cyberspace activities.[22] Here, the international group of experts was split as to whether international human rights treaties that do not explicitly address extraterritoriality nevertheless impose such obligations on the signatories.

From the perspective of any principal actor in the original position, it is difficult to fathom a decision to surrender sovereign options based on restrictions to which they did not expressly agree. The ethical norm acceptable to every state is to operate within the confines of treaty obligations and international law but to also seek additional international frameworks to defend human rights where practicable.

Rule 39: Inviolability of Premises in Which Cyberspace Infrastructure is Located

The international group of experts concluded that cyberspace infrastructure within embassies and consular posts is protected by the inviolability that applies to such diplomatic locations.[23] What was not entirely clear was whether states have an international obligation to respect the inviolability of diplomatic missions or consular posts in *other* states, since the establishment of embassies and the like are primarily based on a bilateral relationship between host and hosted state.[24]

As the anecdote goes, Willie Sutton responded to the question as to why he robbed banks: "That's where the money is." Similarly, diplomatic missions are treasure troves of important information regarding state activity and intent. It is no wonder that Soviet intelligence services positioned electromechanical keyloggers in US embassy typewriters, within Soviet territory no less, during the late 1970s.[25] While the physical inviolability of diplomatic premises is an established international norm, cyberspace inviolability is clearly not consistent with state practice by the primary actors. Any state in the original position would appreciate the utility of nondestructive cyberspace operations within embassies and consular posts to gather intelligence on hosted state motives, activities, and capabilities. Nevertheless, victim states also retain the right to protest whenever such activity is exposed. Ethical cyberspace operations can reasonably include maneuvers within diplomatic premises when carried out without causing damage.

Rule 46: The Right to Visit and Cyberspace Operations

International law establishes that all states have the right to board a vessel on the high seas or in an exclusive economic zone without flag state consent if the vessel is suspected of piracy, slave trading, unauthorized broadcasting, is without nationality, or is of the nationality of the visiting vessel.[26] An interesting, yet unresolved, legal question, is whether a right of visit can be carried out through OCO from the visiting warship.[27]

OCO-enabled virtual visits have some potential to be less invasive than physical searches and pose less physical risk to both crews. On the other hand, a virtual visit is not consistent with the plain text of the law and could actually be more informationally invasive than a physical boarding, since OCO could easily retrieve personal, commercial, and financial files completely irrelevant to determining vessel nationality or confirming maritime criminal activity. While physical maritime visits are both announced and clearly visible, virtual visits could be announced or unannounced. Moreover, any ship threatened in advance of a virtual visit via OCO could naturally take countermeasures, such as powering off noncritical systems. If OCO was successful despite specific countermeasures, that fact, too, could be revealed, making future virtual visits ever more challenging. OCO-savvy states may even be incentivized to operate honeypot vessels designed to incite virtual visits from other states to discover and proliferate novel OCO techniques.

This rule, in particular, highlights the value of the original position in deducing ethical OCO behavior. The specter of military vessels hacking into foreign private and commercial vessels on the high seas under the auspices of right to visit is one that none of the primary actors would find acceptable and is thus unethical.

Rule 122: Perfidy

Perfidy is the use of treacherous deception to kill, injure, or capture an adversary by falsely claiming protected status, and it is prohibited for OCO.[28] The prohibition on perfidy is codified in customary international law for both international and noninternational armed conflict and also appears in Article 23(b) of the Hague Conventions.[29] However, the international group of experts was split as to whether the perfidious act must actually result in adversarial death or injury to be prohibited. ICRC commentary asserts that "it seems evident that the attempted or unsuccessful act also falls under the scope of this prohibition" based on the 1977 Protocol I supplement to the Geneva Conventions.[30] Adding to the complexity of the perfidy issue is that the US is not a signatory to the Protocol I, although China and Russia (and more than 50 other states) are. The contrasting legal viewpoint is that the plain text of the Hague Conventions and Protocol I explicitly describe death, injury, and capture as consequences of prohibited perfidy. Given the inherent deception and secrecy required by all forms of OCO, it is not surprising that scholars have struggled to determine what constitutes perfidy in the cyberspace domain.

USCYBERCOM cannot conduct OCO from publicly-known Internet Protocol addresses at the Pentagon directly against its targets and expect to have any success at all; OCO necessitates masquerading and maneuvering through the "gray space" between friendly "blue" and adversarial "red" cyberspace terrain. Cybersecurity researcher Heather Roff took an uncommon stance on these facts, arguing that OCO erodes the minimal trust necessary between belligerents and that "any use of a cyberweapon that results in the killing, wounding, or capture of an adversary is impermissible."[31] Naval Postgraduate School professor Neil C. Rowe also argued that many forms of OCO involve perfidy.[32] Regarding covert action, under which many OCO may be categorized, former National Intelligence Council chairman Gregory Treverton

wondered how "covert action, even if justifiable. . . can be reconciled with democratic principles," and political theorist Charles Beitz lamented whether "the capacity to conduct covert operations in peacetime should properly belong to the executive branch at all."[33]

Alternatively, many other experts, including Dipert, argue that the OCO makes frequent use of *ruses* rather than *perfidy*, and ruses are permitted under international law. The *Tallinn Manual 2.0* identifies the following examples of OCO ruses: (1) the creation of simulated forces, (2) the transmission of false information to lead the adversary that operations are about to occur, (3) the use of false computer identifiers such as network addresses, (4) feigned OCO not intended to induce terror, (5) bogus orders, (6) psychological operations, (7) transmitting false intelligence, and (8) the use of enemy codes, signals, and passwords.[34] Importantly, the international group of experts reached a consensus on this latter interpretation of ruse versus perfidy in the cyberspace domain, and thus it carries significant weight.

International law, thus, allows for the extensive use of deception and ruses within OCO, but the question remains as to whether or not cyberspace-enabled perfidy that does not kill, injure, or capture is ethically permissible. Here, again, the use of the original-position thought experiment is illuminating; perfidy is prohibited because treachery undermines the value and trust in acts of good faith, such as the raising of a white flag of surrender. No state would endorse perfidy from the original position, lest it be permitted against themselves. Regardless of how tactically advantageous it may be to use OCO to broadcast a false report of a cease-fire to confuse an adversary during an intense armed conflict, such actions, whether they ultimately result in death, injury, or capture, are definitively unethical.

Rules 124–125: Improper Use of the Protective Indicators and UN Emblem

It is prohibited to make improper use of protective indicators that are set forth under the LOAC, such as the American Red Cross and Red Crescent.[35] Likewise, the unauthorized use of the UN emblem is prohibited. The international team of experts approached the application of these rules in cyberspace in two ways. Some experts interpreted the text of the law to narrowly apply to protective indicators such as graphics, while the other experts followed a teleological interpretation that broadly included Internet domain names and text indicators as well.[36] An example described in the *Tallinn Manual 2.0* is that of a phishing email spoofed to appear from the ICRC website to evade adversary email filters; falsified use of the Red Cross domain name in an OCO would be unlawful based on the second legal approach but not to the first.

Under the Rome Statute of the International Criminal Court, intentional attacks against humanitarian assistance personnel are war crimes.[37] Humanitarian relief to civilian populations is essential—both during and after armed conflict—to prevent starvation and provide treatment to the wounded and sick. The ICRC's respected impartiality allowed it to provide 2,100 tons of assistance to thousands of displaced civilians in Crimea throughout 2017.[38] Any operations that undermine trust in the protected nature of humanitarian organizations or the UN fundamentally jeopardize

humanitarian assistance and peacekeeping activities and, therefore, would be considered unethical from the original position by any of the primary actors. The improper use of protective indicators and the UN emblem must be avoided within OCO.

Although not directly related to Rules 124 and 125, the US *Department of Defense Law of War Manual* states that the false use of journalist credentials to feign civilian status to facilitate spying or sabotage is not technically prohibited.[39] The US has not announced any intent to make use of such deceptions in cyberspace, but the perspective of the original position can give leaders insight into the ethical soundness of such deception during the joint planning process. After all, journalists are permitted under international law to obtain identity cards that verify their default status as noncombatants.[40] Would it be ethical to undermine journalist protections under Additional Protocol I, to which the US is not a party, but for which the official US position is that it supports and respects this important principle?[41]

Conclusion

Current military OCO mission planning courses gloss over the LOAC as if it applied perfectly to cyberspace and had resolved all potential ethical quandaries in store for USCYBERCOM. As this article has shown, the legal landscape is more porous than generally appreciated, and the need for ethically-minded leadership is essential in this legal gray zone. Military judge advocate generals tasked to "find a way to yes" for their commanders do so with the privilege of a contemporary—if tenuous—US supremacy in the physical domains of air, land, sea, and space as they provide guidance on legal force projection. Cyberspace is different. In cyberspace, the US is simply one of several principal actors, and additional states are rapidly growing their forces to join the fray. Every experiment sets a precedent as the international norms of behavior codify. The focus should be toward reflective rather than assertive thinking, following the example set forth by the *Montreux Document*. Senior leaders must use ethical reasoning in addition to their legal guidance in the years ahead to ensure that force projection through OCO is made responsibly and sustainably. To these ends, the use of the original-position thought experiment can be a valuable ethical decision-making tool. ✪

Notes

1. George Lucas Jr., "Emerging Norms for Cyberwarfare," in *Binary Bullets: The Ethics of Cyberwarfare*, ed. Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (New York: Oxford University Press, 2016), 27, http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780190221072.001.0001/acprof-9780190221072.

2. Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, MA: Cambridge University Press, 2017).

3. Randall Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9, no. 3 (December 2010): 384–410, http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404.

4. Ibid., 384.

5. Brian Mazanec, "Why International Order in Cyberspace is Not Inevitable," *Strategic Studies Quarterly* 9, no. 2 (Summer 2015): 78, http://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-09_Issue-2/mazanec.pdf.

6. Ibid., 86–88.

7. Lucas, "Emerging Norms for Cyberwarfare," 29–30.

8. John Rollins, "U.S.-China Cyber Agreement," *CRS Insight*, 16 October 2015, https://fas.org/sgp/crs/row/IN10376.pdf.

9. Charlie Dunlap, "Cyber Operations and the New Defense Department Law of War Manual: Initial Impressions," *Lawfare*, 15 June 2015, https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions.

10. Julian Ku, "How China's Views on the Law of *Jus ad Bellum* Will Shape Its Legal Approach to Cyberwarfare," *Hoover Institution*, 17 Aug 2017, https://www.hoover.org/research/how-chinas-views-law-jus-ad-bellum-will-shape-its-legal-approach-cyberwarfare; and International Committee of the Red Cross (ICRC), *The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict* (Geneva: International Committee of the Red Cross, August 2009), 5, https://www.icrc.org/eng/assets/files/other/icrc_002_0996.pdf.

11. Dunlap, *Defense Department Law of War Manual.*

12. Lucas, "Emerging Norms for Cyberwarfare," 17.

13. ICRC, *The Montreux Document,* 5.

14. Ibid.

15. John Rawls, *A Theory of Justice* (Cambridge, MA: Harvard University Press, 1971).

16. Schmitt, ed., *Tallinn Manual 2.0*, 21.

17. Simon Chesterman, "The Spy Who Came in From the Cold War: Intelligence and International Law," *Michigan Journal of International Law* 27, no. 4 (2006): 1129.

18. Schmitt, ed., *Tallinn Manual 2.0*, 55.

19. Ibid., 58.

20. Ibid., 122–23.

21. Ibid., 124.

22. Ibid., 182.

23. Ibid., 212.

24. Ibid., 214.

25. Dan Goodin, "How Soviets used IBM Selectric Keyloggers to Spy on US Diplomats," Ars Technica, 13 October 2015, https://arstechnica.com/information-technology/2015/10/how-soviets-used-ibm-selectric-keyloggers-to-spy-on-us-diplomats.

26. Schmitt, *Tallinn Manual 2.0*, 235.

27. Ibid., 238.

28. Ibid., 491.

29. "Annex to the Convention: Regulations Respecting the Laws and Customs of War on Land—Section II: Hostilities—Chapter I: Means of Injuring the Enemy, Sieges, and Bombardments—Regulations: Art. 23," *ICRC*, https://ihl-databases.icrc.org/ihl/WebART/195-200033?OpenDocument.

30. ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Geneva: Martinus Nijhoff Publishers, 1987): 433, https://www.loc.gov/rr/frd/Military_Law/pdf/Commentary_GC_Protocols.pdf.

31. Heather Roff, "Cyber Perfidy, Ruse, and Deception," in *Binary Bullets: The Ethics of Cyberwarfare*, eds. Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (New York: Oxford University Press, 2016), 202.

32. Randall Dipert, "Distinctive Ethical Issues of Cyberwarfare," in *Binary Bullets: The Ethics of Cyberwarfare*, eds. Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (New York: Oxford University Press, 2016), 68.

33. Charles Beitz, "The Ethics of Covert Operations," *Philosophy and Public Policy Quarterly* 8, no. 4 (1988): 14, https://journals.gmu.edu/PPPQ/article/view/983.

34. Schmitt, *Tallinn Manual 2.0*, 495–96.

35. Ibid., 496.

36. Ibid., 498.

37. ICRC, "Rule 31. Humanitarian Relief Personnel," accessed 1 June 2018, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule31.
38. ICRC, "Assistance to People Displaced in Relation to the Conflict in Ukraine in 2017," 16 January 2018, https://www.icrc.org/en/document/conflict-ukraine-2017-facts.
39. Office of General Council, *Department of Defense Law of War Manual*, June 2015, 307, https://www.defense.gov/Portals/1/Documents/law_war_manual15.pdf.
40. Ibid., 175.
41. Ibid., 174.

Maj Benjamin Ramsey, USAF, PhD

Major Ramsey (PhD, MSEE, Air Force Institute of Technology; MA, US Naval War College; MS, American Military University; BSEE, North Carolina State University) is the director of operations, 352nd Cyberspace Operations Squadron, Joint Base Pearl Harbor–Hickam AFB, Hawaii. Major Ramsey has published more than 40 book chapters, journal articles, and conference papers on wireless network security and critical infrastructure protection. He is also a graduate of the Advanced Strategist Program at the US Naval War College, a certified information systems security professional, and an authority on wireless personal area network security.