AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

# REFINING UNITED STATES POLICY ON OFFENSIVE CYBER OPERATIONS

by

Max C. Johnson, Maj, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

**MASTER OF OPERATIONAL ARTS AND SCIENCES**

Advisor: Lt Col (RAF) Graem M. Corfield

Maxwell Air Force Base, Alabama

November 2014

## Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

# Abstract

This paper examines United States and international policy related to offensive cyber warfare, specifically cyber exploitation and cyber attack. Current domestic and international policies lack mechanisms to classify offensive cyber operations into any discernable categories other than “hostile acts”. Recent cyber-attacks demonstrate how this policy void leads to stark differences in the ways nations perceive the role of the Internet and acceptable conduct in the cyber domain. Moreover, opaque national cyber policies increase the risk states will misinterpret each other’s intentions and actions, leading to inadvertent conflict escalation.

This current policy framework is insufficient to promote international norms or deter adversaries from conducting offensive cyber operations against U.S. networks. This paper advocates using a three variable approach to classify cyber operations based on the actor, the target, and the effect. Examining each variable in depth shows how this classification system would affect broader changes to U.S. and international cyber policy. This new approach could clarify guidance for the United States’ own actions, encourage stability, and promote effective responses to a range of threats from a variety of actors.

Refining United States Policy on Offensive Cyber Operations

Current U.S. policy on offensive cyber operations is too vague to deter attacks or encourage normative international conduct in cyberspace. In order to reduce uncertainty and ensure the most effective responses to hostile cyber-exploitation and attack, the United States should adopt a new method of classifying offensive cyber operations based on three variables: the actor, the target, and the effects. After reviewing current international and United States policies, this paper will articulate the benefits of more comprehensive and transparent guidelines and demonstrate how these variables will shape a new cyber policy.

## Discussion

**Policy Review.** Current international governance on cyber warfare stems from broad interpretation of the United Nations (UN) Charter and application of customary international law. Several nations voluntarily participate in treaties pertaining to cybercrime; however, there is no clear precedent of what activities go beyond crime and constitute an act of terrorism or an act of war.[1] UN Charter Article 2(4) prohibits nations from “the threat or use of force against the territorial integrity or political independence of any state.”[2] Articles 29 and 42 contain two exceptions to this prohibition, authorizing force in response to “any threat to the peace, breach of the peace, or act of aggression” and to “maintain international peace and security.”[3] Article 51 also recognizes a state’s right to use force for its “inherent right of individual or collective self-defense.”[4] However, nowhere does the UN Charter define what constitutes a “use of force, “threat” of force, or an “armed attack.” [5] Concerning self-preservation, the UN is equally vague, stating only an attack must be “instant” and “overwhelming” before a state can invoke its inherent right of self-defense.[6] Without clear international law or established norms, states, organizations, and individuals are left on their own to determine what constitutes acceptable conduct. This creates an environment in which enemies and allies alike are unclear how their actions will be interpreted and what behavior they can reasonably expect from others.

The vacuum of formalized cyber policy leads to stark differences in how nations perceive the role of the Internet and acceptable conduct in the cyber domain. The United States traditionally views the Internet as a “global commons” and therefore emphasizes the importance of access, privacy, and freedom of speech.[7] However, other actors take a fundamentally different view. China and Russia (the United States’ near-peer cyber competitors) view the free flow of information as a threat to domestic stability.[8] Consequently, China focuses as much on restricting content for its domestic users as it does on information warfare and reconnaissance of foreign websites.[9] Shaped largely by its perceived loss of the information operations campaign in the Cold War, Russia’s primary concern is managing information flow and securing its own communications networks.[10] These vastly different perspectives encourage conduct other states consider unacceptable. For example during a 2008 succession conflict, Russia conducted a 19-day denial-of-service attack against Georgia, effectively blocking government, transportation, media, and financial sector Internet access.[11] More recently, the Chinese government targeted its own citizens, blocking pro-democracy content related to protests in Hong Kong.[12] Given these fundamentally disparate perspectives, it is unlikely the international community will reach consensus on cyber policy in the near future. Baring a multilateral agreement, each state must independently convey what actions it considers acceptable and off-limits.

Like the UN Charter, current U.S. cyber policy is too vague to provide predictability or encourage normative behavior. Due in part to limited understanding and compartmented classification, cyber policy is not well integrated into the United States’ overall strategic plans.[13] The primary open-source document for U.S. cyber policy is the 2011 International Strategy for

Cyberspace. In mostly non-specific terms, this strategy describes a policy aimed at promoting free speech, privacy, and the free flow of information both domestically and abroad.[14] The policy addresses threats from criminals, terrorists, and states, but stops well short of defining what actions constitute crimes, terrorism, and acts of war. Moreover, the document makes no distinction in how to manage these unique threats, stating simply that the United States will respond to hostile acts in cyberspace with "a range of credible response options"[15] and "all means…as appropriate and consistent with international law."[16] Nowhere does United States policy publically define what options are considered "credible" or "appropriate" or what "hostile acts" would trigger a response. The International Strategy for Cyberspace does identify transportation, financial systems, digital infrastructure, and the defense industrial base as "critical infrastructure", but only in terms of their need for defense.[17] The White House avoids stating whether it considers attacks on networks to be off-limits or what adversaries should expect if they conduct operations against U.S. critical infrastructure.

Despite its many shortcomings, current U.S. national strategy does recognize the need for international cyberspace norms. In addition to extending traditional American values to cyberspace, the International Strategy identifies important emerging norms like network stability, reliable access, and cyberspace due diligence.[18] Regarding conduct in cyber warfare, United States policy advocates extending customary international law to cyberspace.[19] While this is an important statement, it lacks any discussion of how existing international laws should be applied to the cyber domain. Addressing and publicizing these critical policy gaps will significantly benefit all Internet users and nations in general, and the United States in particular.

**Benefits of Redefined Policy.** In all forms of warfare, states risk misinterpreting the intentions and actions of their adversaries, thus evoking disproportionate responses and inadvertently escalating a conflict. Offensive cyber warfare is especially prone to this phenomenon because benign or minimally provocative actions often look identical to massive attacks.[20] All offensive cyber activities involve three basic components; a vulnerability, a point of access, and a payload.[21] After gaining access to a system through an identified vulnerability, the attacker implants a payload to achieve their desired effects. Whether the payload is designed to passively observe activity, destroy data, or sabotage critical infrastructure, offensive actions depend on the same vulnerabilities and access points. Therefore, after identifying an intrusion, the network owner will not know the attacker's intentions unless they find and accurately reverse-engineer the payload. Moreover, engineers can design payloads with two or more purposes. These viruses can wait on a network passively collecting data for years until the intruder activates a destructive attack.[22] This ambiguity predisposes network owners to assume every intruder has seriously malicious intentions, thus increasing the potential for rapid conflict escalation. Clear national policy helps mitigate this misunderstanding by giving potential enemies a sense of what actions will elicit a particular level of response.[23] Publicizing and adhering to a standard of conduct establishes a baseline behavior from which others can interpret your actions. Historically, sharing standard operating procedures diminishes misunderstandings and enhances mutual security between allies and adversaries.[24] All nations, especially the United States, stand to benefit from minimizing conflict escalation through clear understanding of national cyber policies.

More than any other country, the United States has a significant asymmetry between its reliance on cyberspace and its vulnerability to a cyber-attack. As an early Internet adopter and a technologically advanced society, the United States has a greater dependency on cyber controlled systems than most other nations.[25] The U.S. military, economy, government, and citizens are wired to and operate through the Internet, leaving very few networks immune to a cyber-attack. Also, unlike many other countries, politically powerful corporations own many of the United States' most essential systems and infrastructure.[26] Where other nations can force compliance with security best practices or isolate infected networks, the United States government has comparatively little authority to direct security for financial institutions, the national electrical system, defense contractors, or hospitals. Finally, the United States military itself is more reliant on cyber technologies than its peer and near-peer competitors.[27] Given this imbalance between its dependence and vulnerability, the United States has a compelling interest to advance international norms for cyber warfare. Coupled with this interest, the United States also has more authority to promote cyberspace norms than any other state or non-state actor. America's superpower status, allure as a cyber target, and demonstrated offensive cyber capability make it uniquely qualified to champion international cyber policy. The actions and positions the United States takes today will set precedents for international conduct for the foreseeable future.[28] Given the ambiguity of international law and differences of opinions on the fundamental use of the Internet, the United States must clarify its own policy to establish precedents and promote stable behavior.

**Classification System.** The primary deficiency of current United States cyber policy is that it makes no differentiation between various kinds of actions or actors. The 2011 International Strategy for Cyberspace effectively lumps theft by criminal organizations, espionage by states, and acts of violence by terrorists under the broad category of "hostile acts." This indiscriminate approach gives no guidance for U.S. offensive operations, provides no deterrent to adversaries, and promotes no normative behavior aimed at reducing conflict escalation. To encourage transparency and stability, the United States should adopt a method of classifying hostile cyber activities along three variables: the actor, the target, and the effects. This approach will encouraged tailored threat responses, establish a baseline for normative behavior, and provide clear guidance for U.S. offensive cyber operations.

**Actor.** The first variable for a new classification system is the actor, or source of the action. United States cyber policy must differentiate between criminal, terrorist, and state sponsored cyber actions and promote norms that encourage accurate attribution. More than any other operating environment, actors in cyberspace can achieve strategic effects and inflict damage disproportionate to their size or resources.[29] However, this does not imply that the United States can cooperate with or retaliate against all of these unique actors using the same paradigms and tools. While nation states may respond to traditional instruments of power and might be willing to enter multilateral agreements, non-state actors are certainly less susceptible to these classic geopolitical strategies.[30] Considering cyber-crime's global nature, the United States must deter, investigate, and prosecute cyber-crimes through local national laws in cooperation with other governments.[31] However, the United States will need to address state-sponsored cyber threats with a very different set of tools ranging from diplomacy to kinetic strikes. Categorizing attacks by actor will ensure the United States uses tailored and effective responses to cyber-attacks, rather than the current one-size-fits-all approach.

Unfortunately, identifying the source of a cyber-attack is not always easy since cyber operations lend themselves to anonymity. Skilled cyber operators can mask their identities behind multiple servers located across the world. Using software to trace-back an attack often leads to a dead-end server. Depending on their level of cooperation and technical competence, host nation law enforcement assistance will certainly take time and may not be effective.[32] In fact, skilled hackers often route their attacks through states with whom they know their target has poor diplomatic relations.[33] Further complicating the attribution problem, some states are known or suspected of sponsoring nationalistic civilian hackers to distance the government from the attack and provide some measure of plausible deniability. Chinese Information Warfare doctrine points to the use of civilian hackers to carry out a “people’s network war” in conjunction with national military or diplomatic campaigns.[34] While not officially sanctioned by their governments, hackers in Russia, Israel, and Palestine have also conducted attacks in furtherance of their nation’s strategic goals.[35] However difficult attribution may be, it is a necessary requirement to promote stability and lawful cyber warfare.

Identifying oneself is an essential condition of the Laws of Armed Conflict. Both the Geneva and Hague conventions prohibit perfidy, or acts of treachery.[36] Examples of perfidy include falsely claiming noncombatant status and deceiving your enemy through a faux surrender. Perfidy is considered so reprehensible because it undermines the basic trust necessary to conduct lawful war.[37] States that mask their identity or use civilians to conduct their cyber-attacks are also guilty of undermining this trust. Without the ability to identify one’s attacker, states can have no confidence in their treaties or trust the intentions of their friends or enemies.[38] Attribution is especially important in cyberspace because attacks are so often invisible to the outside world. Without media coverage, aid workers, or UN inspectors to see the impacts of a cyber-attack, the reputations of the parties involved weigh very heavily on how the world interprets one’s actions.[39] To establish a reputation as a responsible cyber superpower and promote norms that allow states to attribute attacks to their source, the United States must set a precedent of taking credit for its own actions in cyberspace. Operational necessities will obviously preclude announcing offensive cyber actions in advance or even taking credit for them immediately after an attack. However, the United States must claim responsibility for cyber-attacks before the targeted entity can misinterpret its intentions and inadvertently escalate to a higher level of conflict.

In addition to taking credit for cyber operations, the United States should publically renounce the use of state-sponsored civilian hackers. Most modern nations regard state-sponsored terrorism as morally reprehensible in part because it uses non-combatants in a military capacity and ignores the requirement to claim responsibility for one's actions.[40] Publically, other states will likely deny any connection to civilian hackers and in some cases, may truly be incapable of controlling independent civilians motivated by patriotism. It is still unclear whether China actually sponsored civilian-run cyber offensives against Japan and Taiwan and it is plausible that both attacks originated from China's highly nationalistic population without government encouragement. [41] In these cases, the United States should insist on transparency and cooperation, seeing what the host nation has done to prevent civilian attacks and allowing international intervention to stop them.

Classifying cyber-attacks by actor will ensure the United States employs the appropriate tools and makes the most effective responses to hostile acts. Pursuant to this strategy, the United States must set a precedent of claiming credit for its own actions and insisting that other states do the same. While attribution in is not always easy, it is absolutely essential for lawful conduct in war and necessary to promote stability in cyberspace. Finally, the United States must condemn the use of state-backed civilian hackers. These partnerships further complicate the attribution problem and violate international laws requiring distinction between civilians and combatants.

**Target.** United States policy must also differentiate between offensive cyber operations based on the action's target. Currently, there exists no international agreement on what objects are considered valid military targets under the Laws of Armed Conflict.[42] Therefore; states must use their own discretion in applying principles like distinction, necessity and proportionality. Moreover, non-state actors undeterred by UN resolutions or world opinion may opt to disregard international norms altogether and attack any target necessary to meet their goals. A 2008 Central Intelligence Agency report cited several cases of hackers targeting national electrical systems and ransoming the affected government before restoring service.[43] In this ambiguous environment, the United States should proactively identify networks it considers off-limits to cyber-attack. Without enumerating specific targets or listing exact consequences, the United States can identify broad categories of networks, which if attacked, will evoke a more serious response than a similar action against a non-critical network. This policy would serve both as a guide for the United States' operations and as a deterrent for its adversaries.

The current United States International Strategy for Cyberspace lists energy, transportation, financial systems, and the defense industrial base as "critical infrastructure" and also describes information systems as "vital national assets".[44] However, the document stops well short of providing any guidance regarding attacks against these networks. State and non-state actors alike conduct daily intrusions and low level attacks on financial networks, the national power supply, and U.S. defense contractors.[45] Clearly, the United States cannot and should not respond to each of these intrusions and attacks in the same manner. Publically designating critical infrastructure as a kind of "digital safe haven" sets expectations of behavior while still leaving room to tailor a response to the specific action.[46] Even without knowing the exact consequences, criminals, terrorists, and governments alike will reevaluate the prudence of attacking U.S. critical infrastructure if assured their actions will evoke a serious response. Revised policy should also state that the United States will not attack another nations' critical infrastructure except during times of war and after careful consideration of the Laws of Armed

Conflict. This declaration will improve transparency and perceived legitimacy of U.S. cyber policy.

Even careful target selection and a well-intentioned policy aimed at avoiding conflict escalation cannot mitigate all the unforeseen consequences of cyber-attacks. Unlike kinetic weapons with finite lethal and collateral effects ranges, cyber weapons have the potential to inflict damage well beyond their intended target. Unknown or new network configurations and software changes can easily cause cyber-attacks to migrate onto collateral systems or applications.[47] For example, an attack aimed at an enemy's air defense network may affect other functions of their national or even regional air traffic control system, creating unacceptable hazards to civilian flight. Although not publically acknowledged, strong evidence suggests the 2010 Stuxnet virus, originally designed to attack Iran's nuclear enrichment program, migrated onto tens of thousands of computers via a hole in the Windows operating system.[48] Given this risk of collateral damage, senior policy makers must carefully consider the potential costs and benefits of an attack within the broader geopolitical context. Based on this analysis, national leadership may decide to avoid cyber-attacks on particular targets or choose smaller attacks with more modest outcomes.[49] Therefore, senior policy leaders should retain approval authority for offensive cyber operations potentially affecting another nation's critical infrastructure. These well-informed national leaders must be prepared to manage the political repercussions of an attack's collateral damage.

**Effects**. Along with the actor and the target, United States cyber policy must classify cyber actions by their intended and actual effects. Simply qualifying all cyber operations by terrorist organizations as an act of terror or all intrusions into critical infrastructure as an act of war is an impractical oversimplification. Key policy issues related to effects include differentiating between cyber-attacks and cyber-exploitation; confronting sabotage and covert military action; and addressing unintended and collateral effects.

Current United States policy makes no distinction between cyber-attack and cyber-exploitation. Cyber-attack involves actions to destroy, degrade, disrupt, or deny an enemy's information or information networks. Conversely, cyber-exploitation is non-destructive, involving the smallest possible intervention to obtain information that would otherwise be confidential.[50] While national policy is unclear how the United States views these very different activities, international customs related to espionage do provide some guidance useful for confronting cyber-exploitation. Like espionage, cyber-exploitation seeks to obtain information (clandestinely if possible) without destroying or altering it. No international law exists to prevent espionage because of the implied understanding that all states do it and that spying provides insight contributing to stable international relations. Acts of espionage therefore are considered crimes rather than acts of war and are governed by domestic rather than international laws.[51] A mature U.S. cyber policy could easily extend this precedent to the cyber domain by stating that the United States will respond to cyber-exploitation with its existing domestic laws for corporate and government espionage. Aside from deterring network intrusions, this approach would also minimize the potential for escalatory behavior. Undoubtedly, the United States and other nations will find it necessary to engage in cyber-exploitation in the future. Establishing the precedent that these incidents, while provocative, do not constitute acts of war, will encourage state actors to respond through legal and diplomatic channels rather than military action.

Offensive actions that go beyond espionage, but stop short of a destructive attack pose an even greater challenge to effects based classification. Depending on the actor and target, these actions are tantamount to sabotage or covert military action and could very easily be considered an act of terrorism or act of war.  In 2009, Chinese hackers implanted logic bombs in network controllers tied to the U.S. power grid.  While the destructive payload was never activated, this action had the same practical effect as rigging high-tension power lines with remotely detonated explosives.[52]  Surprisingly, the incident elicited very little attention, particularly considering the equivalent action in the physical domain (rigging explosives) would arguably warrant a strong political or military response.  United States cyber policy must unequivocally state that it will judge and respond to cyber-attacks based on their equivalent effects in the physical domain.  This stance is consistent with the Laws of Armed Conflict, which judge an action's legality based principally on its effects rather than its modality.[53]  Deploying a virus designed to disable satellite communications is no less hostile an act than attempting to physically destroy the satellite's ground control terminal.  This is a critical shortfall of current U.S. cyber policy and a key element necessary to shift international norms and deter attacks.

The aforementioned possibility of collateral damage complicates, but does not preclude, effects-based classification.  A cyber-attack with relatively limited intended effects may migrate onto collateral networks or cause more destruction than originally designed.  While collateral damage is an unavoidable consequence of war, combatants are nonetheless responsible for both the intended and unintended results of their actions.  Article 51 of the 1977 Additional Protocol to the Geneva Conventions prohibits attacks "whose effects cannot be controlled" and mandates belligerents take constant care to mitigate harming civilian persons and objects.[54]  Consistent with these precedents, U.S. cyber policy should state that it holds attackers accountable for their actions' primary and collateral effects.  This further supports the argument for centralizing offensive cyber activity under the authority civilian government leaders with the coordination of military advisors. National leaders must understand the likely and possible outcomes of various cyber-attacks and be prepared to manage their unintended collateral consequences.

## Conclusions

In its current form, U.S. cyber policy is too vague to promote international norms, prevent inadvertent conflict escalation, deter cyber-attacks, or tailor effective responses to various cyber threats. As a superpower and cyber-reliant nation, the United States is uniquely positioned to affect and benefit from stability in the cyber domain. The United States can begin to address these issues by publically adopting a system of classifying offensive operations by their actor, their target, and their effects. This framework would not only serve to categorize threats to domestic information networks, but would provide guidance for U.S. offensive cyber operations.

With regard to the actor or source of attack, the revised U.S. International Strategy for Cyberspace should differentiate between criminal, terrorist, and state activity. The United States has a variety of laws and organizations uniquely tailored to confront criminals, terrorists, and foreign militaries. Distinguishing between cyber-crime, cyber terror, and cyber warfare will ensure the United States pursues the appropriate partnerships and employs the most effective tools to address these diverse threats. Moreover, proper attribution is an essential element of lawful warfare. In accordance with the Laws of Armed Conflict, U.S. policy should condemn state sponsored civilian hackers and encourage states to take credit for their actions. To establish this norm, the United States must claim responsibility for its own offensive activities as soon as operationally feasible. This behavior will improve transparency and mitigate unintended conflict escalation.

To establish a baseline of acceptable behavior and discourage attacks against its critical infrastructure, U.S. policy must also classify attacks according to their target. While it is impractical and ill advised to identify specific network nodes or list exact responses to every attack, revised policy should posit broad classes of critical infrastructure the United States considers “off limits.” This distinction signals to adversaries that attacks and intrusions against these networks will evoke a higher level of response than similar actions against non-critical targets. To provide legitimacy to this policy, United States must hold itself to the same standard and refrain from attacking another nation’s critical infrastructure except during times of war and after due consideration of the Laws of Armed Conflict. This conduct will help establish precedents for responsible behavior currently lacking in international law.

A revised U.S. policy should also distinguish between attacks based on their effects. The current approach of lumping all offensive cyber activity under the umbrella of “hostile acts” exaggerates the gravity of some actions while grossly understating the significance of others. The United States must first distinguish between cyber-exploitation and cyber-attack. Both the intent and effects of cyber-exploitation are very similar to espionage. Cyber-exploitation therefore is best regulated by domestic laws and resolved via legal and diplomatic channels rather than through military action. Regarding cyber-attack, the United States should compare the practical effects of an attack with equivalent actions in the physical domain. Planting a virus intended to disrupt the national power supply should evoke the same response as placing explosives in electrical plants or on power lines. While international law does not preclude collateral damage, it does hold belligerents responsible for their actions’ secondary effects. Consistent with this principle, cyber policy should unequivocally state that actors are responsible for their attacks primary and collateral effects.

## Recommendations for Future Study

Future research should investigate methods for providing political oversight while still enabling timely and flexible cyber operations. Cyber activity is very susceptible to misinterpretation and is particularly prone to inadvertent conflict escalation. Moreover, cyber-attacks often have unknown but profound secondary effects and can easily migrate from their intended target onto collateral objects. International policy and norms are not yet clear enough to suggest how other states will respond to cyber-attacks and intrusions. U.S. leadership must consider potential political repercussions without unnecessarily restricting cyber operations. Further investigation is necessary to determine the appropriate approval authority for various cyber-attacks, the approval process, and the advisory positions necessary to educate political leadership on offensive capabilities and limitations.

1. Wayne Henry, Jacob Strange, and Eric Trias, “Pearl Harbor 2.0: When Cyber –Acts Lead to the Battlefield.” Proceedings of the International Conference on Information Warfare and Security (2010): 148, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=49549154&site=ehost-live&scope=site&custid=airuniv.

2. Herbert S. Lin, “Offensive Cyber Operations and the Use of Force.” *Journal of National Security Law & Policy*, vol 4:63 (2010): 71.

3. Ibid.

4. Ibid.

5. Ibid., 72.

6. Henry, “Pearl Harbor 2.0,” 152.

7. Adam Segal, “Cyberspace Governance: The Next Step.” *Council on Foreign Relations, Policy Innovation Memorandum*, no. 2 (14 November 2011): 2, http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

8. Ibid.

9. Timothy L. Thomas, “Nation-state Cyber Strategies: Examples from China and Russia.” *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009): 465.

10. Ibid.

11. Jonathan C. Rice, “Core Questions for Cyber-attack Guidance.” *Joint Force Quarterly*, no. 71 (2013): 35, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=91965202&site=ehost-live&scope=site&custid=airuniv.

12. Madison Park, “China’s Internet Firewall Censors Hong Knong Protest News.” *CNN* (30 September 2014), http://www.cnn.com/2014/09/29/world/asia/china-censorship-hong-kong/.

13. Franklin D. Kramer, “Cyberpower and National Security: Policy Recommendations for a Strategic Framework.” *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, D.C.: National Defense University Press, 2009): 14.

14. White House, *International Strategy for Cyberspace* (May 2011): 5, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

15. Ibid., 12.

16. Ibid., 14.

17. Ibid., 19.

18. Ibid., 10.

19. Ibid., 9.

20. Herbert S. Lin, “Escalation Dynamics and Conflict Termination in Cyberspace.” S*trategic Studies Quarterly*, 6.3 (2012): 52, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=84626760&site=ehost-live&scope=site&custid=airuniv

21. Lin. “Offensive Cyber Operations and the Use of Force.” 64.

22. Lin. “Escalation Dynamics and Conflict Termination.” 49.

23. Segal, “Cyberspace Governance.” 1.

24. White House, *International Strategy for Cyberspace*, 21.

25. Richard A. Clarke and Robert K. Knake, *Cyber War* (New York, NY: HarperCollins Publishers, 2010): 227.

26. Ibid.
27. Ibid.
28. Rice, “Core Questions for Cyber-attack Guidance.” 37.
29. Mary M. Manjikian, “From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik.” *International Studies Quarterly*, no. 54.2 (2010): 386, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=51249037&site=ehost-live&scope=site&custid=airuniv.
30. Kramer, “Cyberpower and National Security,” 15.
31. White House, *International Strategy for Cyberspace*, 13.
32. Clarke, *Cyber War*, 226.
33. Henry, “Pearl Harbor 2.0.” 148.
34. Manjikian, “From Global Village to Virtual Battlespace.” 393.
35. Manjikian, “From Global Village to Virtual Battlespace.” 393; Thomas, “Nation-state Cyber Strategies,” 475.
36. Patrick Lin, Fritz Allhoff, and Niel C. Rowe, “Computing Ethics War 2.0: Cyberweapons and Ethics.” *Communications of the ACM*, vol 55, no. 3 (2012): 26, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=73047214&site=ehost-live&scope=site&custid=airuniv.
37. Ibid.
38. Segal, “Cyberspace Governance.” 2.
39. Lin. “Escalation Dynamics and Conflict Termination.” 55.
40. Lin, “Computing Ethics War 2.0.” 26.
41. Thomas, “Nation-state Cyber Strategies.” 466.
42. Henry, “Pearl Harbor 2.0.” 148.
43. Ibid., 152.
44. White House, *International Strategy for Cyberspace*, 12, 19.
45. Lin. “Escalation Dynamics and Conflict Termination.” 66.
46. Segal, “Cyberspace Governance.” 3-4.
47. Rosemary M. Carter, Brent Feick, and Roy C. Undersander. “Offensive Cyber for the Joint Force Commander.” *Joint Force Quarterly*, no. 66 (2012): 26.
48. David E. Sanger, *Confront and Conceal* (New York, NY:Crown Publishing Group, 2012): 203.
49. Lin. “Escalation Dynamics and Conflict Termination.” 65.
50. Lin. “Offensive Cyber Operations and the Use of Force.” 63.
51. Ibid., 72
52. Clarke, *Cyber War*, 198.
53. Lin. “Offensive Cyber Operations and the Use of Force.” 73.
54. Horst Fischer. “Collateral Damage.” *Crimes of War* (2011), http://www.crimesofwar.org/a-z-guide/392/.

## Bibliography

Carter, Rosemary M., Feick, Brent, and Undersander, Roy C. "Offensive Cyber for the Joint Force Commander." *Joint Force Quarterly*, no. 66, 2012: 22-27.

Clarke, Richard A. and Robert K. Knake. *Cyber War*. New York,NY: HarperCollins Publishers, 2010.

Fischer, Horst. "Collateral Damage." *Crimes of War*. 2011, http://www.crimesofwar.org/a-z-guide/392/.

Henry, Wayne, Strange, Jacob and Trias, Eric. "Pearl Harbor 2.0: When Cyber –Acts Lead to the Battlefield." Proceedings of the International Conference on Information Warfare and Security, 2010: 148-154, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=49549154&site=ehost-live&scope=site&custid=airuniv.

Kramer, Franklin D. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington, D.C.: National Defense University Press, 2009: 3-23.

Lin, Herbert S. "Escalation Dynamics and Conflict Termination in Cyberspace." S*trategic Studies Quarterly*, 6.3, 2012: 46-70, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=84626760&site=ehost-live&scope=site&custid=airuniv.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy*, vol 4:63, 2010: 63-86.

Lin, Patrick, Fritz Allhoff, and Niel C. Rowe. "Computing Ethics War 2.0: Cyberweapons and Ethics." *Communications of the ACM*, vol 55, no. 3, 2012: 24-26, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=73047214&site=ehost-live&scope=site&custid=airuniv.

Manjikian, Mary M. "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik." *International Studies Quarterly*, no. 54.2, 2010: 381-401, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=51249037&site=ehost-live&scope=site&custid=airuniv.

Park, Madison. "China's Internet firewall censors Hong Knong protest news." *CNN*, 30 September 2014, http://www.cnn.com/2014/09/29/world/asia/china-censorship-hong-kong/.

Rice, Jonathan C. "Core Questions for Cyber-attack Guidance." *Joint Force Quarterly*, no. 71, 2013: 32-39, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=mth&AN=91965202&site=ehost-live&scope=site&custid=airuniv.

Sanger, David E. *Confront and Conceal*. New York,NY: Crown Publishing Group, 2012.

Segal, Adam. "Cyberspace Governance: The Next Step." *Council on Foreign Relations, Policy Innovation Memorandum*, no. 2, 14 November 2011, http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

Thomas, Timothy L. "Nation-state Cyber Strategies: Examples from China and Russia." *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Washington, D.C.: National Defense University Press, 2009: 465-488.

White House, *International Strategy for Cyberspace*, May 2011, 5, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.