Three Conditions for Cyber Countermeasures

Opportunities and Challenges of Active-Defense Operations

Dr. Nori Katagiri

ABSTRACT

This article explores a variety of opportunities and challenges with the use of cyberspace countermeasures. It critically assesses a set of conditions under which countermeasures can be an appropriate means of offensive cyber: limited aim of defense and deterrence, protection of critical infrastructure, and compliance with rules of behavior. Here, the article shows that countermeasures must be taken for the purpose of active defense and deterrence. Second, they can be appropriate as a means of defending critical infrastructure. Finally, they should be executed by state actors who comply with existing principles of cyberspace behavior. While cyberspace countermeasures can become a socially accepted, legitimate means of active defense and deterrence, the article shows that there are several challenges connected with each of these conditions. For one, there are various degrees of feasibility about what conditions are appropriate for countermeasures. The article also discusses inherent problems in the application of international law, from which rules of engagement are drawn, to cyberspace. The challenges are hard to solve, which may explain why it has been so difficult for the international community to produce a set of agreeable criteria for active defense measures.

Nori Katagiri is associate professor of political science and coordinator of international studies at Saint Louis University. He is the author of *Adapting to Win: How Insurgents Fight and Defeat Foreign States in War*, published by the University of Pennsylvania Press. His works on cybersecurity have appeared in the *Journal of Cybersecurity*, *Global Studies Quarterly,* and *Asian Security,* among other venues. He is a senior fellow at the Irregular Warfare Initiative of the Modern War Institute, United States Military Academy at West Point. Before joining Saint Louis University, he was associate professor of international security studies at the Air War College, a graduate military school of the United States Air Force. He received his Ph.D. in political science from the University of Pennsylvania and served as visiting fellow at the Modern War Institute at West Point, Japan's Air Staff College, Taiwan's National Defense University, and the University of the Philippines – Diliman.

INTRODUCTION

In recent years, experts have paid growing attention to the need to develop a whole new range of countermeasure options to deter hostile acts in cyberspace. This is a healthy development, as well as a reflection of hackers' increasing capabilities and frequency of attacks. As such, the call for an enhancement of defensive measures to counter the trend is long overdue. Yet it is not entirely clear what makes countermeasures appropriate in cyber operations from the standpoint of legal, ethical, society, and strategic effect standpoints. This article will address the three conditions that need to be met for countermeasures to be an appropriate means of cyber operations and explore both the opportunities and challenges of countermeasures. This article places greater emphasis on the strategic and political aspects of conducting countermeasures in cyberspace than other dimensions, such as legal.

First, countermeasures must be planned and carried out for the purpose of active defense and deterrence. Second, they can be appropriate to defend critical infrastructure. Finally, they should be executed by state actors who comply with existing principles of cyberspace behavior. The second part of this argument is that there are various degrees of feasibility with each of the three conditions. The first two conditions are more practical than reliance on norm compliance. It is also important to note that, while the three conditions do not necessarily represent an exhaustive list of opportunities, challenges, and limitations, they serve as a set of necessary factors for the option of countermeasures to be socially accepted and effectively executed. However, because the conditions are not something that can be easily met, not every country will be able to meet the criteria.

The scope of analysis

In cyberspace, countermeasures consist of several types of measures, including "honeypot" (trapping

attackers for forensic analysis), "dye-packs" (tracing seekers of decoy files), and "hacking back" to neutralize stolen data and disable launch servers. The definition allows us to treat countermeasures as a strategic option whose use would be consistent with some of the most important principles of cyberspace behavior, including proportionality and compliance with international law. However, it does not allow us to differentiate countermeasures from other forms of cyber operations. For instance, how are our countermeasures distinguished from offensive cyber operations (OCO), defined here as "missions intended to project power in and through cyberspace"?[1] How do we know which comes first: enemy attacks ("another State's unlawful action") and countermeasures when enemy attacks are frequent and inconsistently responded to? How can we explain the timing and sequence of actions? Public discourse continues to progress under the assumption that answers to these questions would eventually be found.

In this article, countermeasures are defined as a set of responses toward verified attackers within a reasonably short period of time. Countermeasures differ clearly from unprovoked attack operations because they are a response to strikes launched unjustifiably. Instead, countermeasures are a subset of active defense activities, which include a wider set of actions like indictments and sanctions against attackers.[2] Active defense is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of such threats. It differs from passive defense, which involves a wide range of key tasks to reject incoming attacks through security patches, backups, warning systems, and education.[3] The differences are subtle, however, between countermeasures because these actions often occur simultaneously. In fact, except for the unprovoked offensive missions, the defensive measures are in a relationship of mutual reinforcement. Countermeasures are part of key discussions on some of the most recent policies to deal with cyberspace vulnerability. Conceptually, countermeasures are utilized as part of the existing cyber toolkits under the US policy of persistent engagement and defend forward, where the US would closely observe the planning of adversaries and inform partners to take action themselves.[4] Although not explicitly stated, countermeasures can be conducted as an active defense component within a broader cyber defense framework; persistent engagement is partly designed to counter adversaries' measures to attack US infrastructure as a means to help develop their own countermeasures.[5]

Technologically capable states have developed expertise within their bureaucracies and worked with the private sector to devise plans to develop options individually. Collective countermeasures give additional options to countries with similar threat perceptions, although those are mostly already in formal alliances.[6] For instance, within NATO, experts have worked on collective options for some time, a development that may encourage allies elsewhere to consider similar options.[7] However, a horizontal spread of collective countermeasures would take time because in reality, few cyber-active states are in such a privileged position as NATO. Many US defense-treaty allies in the Indo-Pacific, such as Japan and the Philippines, have not yet entered

serious discussions about building a joint architecture, largely because their networks are less integrated and because their alliances with the US are bilateral, rather than multilateral.[8] Even within NATO, there have been calls for restraint against the immediate adaption of its collective defense clause to cyberspace. This is because, according to Jeppe Jacobsen, to do so would risk "undermining the cyber-intelligence norm that so far has prevented escalation and thereby increasing the likelihood that Russia misinterprets intelligence and active cyber defense activities as military preparation, armament or an attack in the making."[9] This discussion underscores the existence of various degrees of acceptability of collective countermeasures.

It is also important to note that while the private sector, especially technology and consulting industries, plays an integral part of countermeasure research and development, only states, and collective defense mechanisms like NATO, would let private actors be justifiably involved in *defensive* measures but not deploy offensive measures.[10] This is due to the fundamental difference between private and public sectors about their basic functionality. Private businesses operate according to financial logic, while governments have national security responsibilities and are under constant scrutiny on how they execute these responsibilities. As a result, most states refrain from engaging private companies directly in attacking foreign servers.[11]

The literature on cyber countermeasures is expanding, with political scientists exploring the functionality of measures like hacking back as a set response to security incidents.[12] Many in private business have explored offensive cyber techniques for financial gains and investment opportunities.[13] Policymakers have increasingly accepted countermeasures as a topic of consideration, possibly more so than the concept of offensive cyber itself. Yet the cyber community has not figured out how to conduct offensive cyber responsibly while minimizing the negative consequences it may cause, such as escalation of tension.[14] There are technical challenges that need to be addressed, too, including how to design and oversee operations and test tools before launching while preventing criminal and third-party access to backdoors.[15] There are three important conditions that should be met as we move forward with the discussion on countermeasures in the framework of offensive cyber.

1. Limited aim of defense and deterrence

The first condition for countermeasures is that they be used not for the purpose of preemption but for defense and deterrence through retaliation and punishment. Countermeasures are most permissible when launched as an act of denying and dissuading future attacks by threatening to impose costs on attackers. The active-defense use of countermeasures is meant to mitigate the persistent failure of the current preventive mechanism to discourage the global proliferation of hostile cyber operations. The spread of malware has accelerated to such a great degree as more malicious actors develop offensive capabilities and gain access to various hacking tools.[16] Countermeasures should then impose reasonable amounts of pain to deter potential attackers. At the same time, countermeasures must be clearly delineated from unprovoked OCO, defined above.

As such, restraint is a critical condition for countermeasures. To make them solely used for the purpose of defense and deterrence, however, actors must meet several sub-conditions. First, countermeasures must be declared publicly, rather than threatened opaquely. Policymakers need to clarify conditions under which they would act defensively and carry through the process to keep their actions credible. When properly executed, declaratory countermeasures allow policymakers to avoid so-called "gray zone" situations and keep attackers from abusing the opaqueness to their advantage by way of plausible deniability.

Second, policymakers need to know that cyber defense and deterrence is hard, with the latter likely harder. Defense and deterrence, respectively, call for different requirements. On the one hand, countermeasures for defensive purposes presume that policymakers, presumably through expert intermediaries, (1) know of the existing vulnerabilities in their systems; (2) can detect an attack and attribute reasonably quickly; (3) know that defense without countermeasures would be insufficient because defense alone has no "teeth." These criteria are already challenging for technical, legal, and political reasons.[17] Only a small number of states have the technological prowess to launch countermeasures in this situation. On the other hand, it is extremely difficult to draw clear effects from countermeasures launched for *deterrence*. Deterrence is invisible; we do not see a thing move when deterrence works. In effect, when a cyber-attack is thwarted, we are tempted to assume that deterrence is not responsible for the lack of action. This is especially tempting because most states accused of perpetrating cyber operations typically do not confirm or deny responsibility.[18] Michael Fischerkeller and Richard Harknett contend that "the protection ... of national interests cannot rest on deterrence as the central strategy" and call for the use of active cyber operations to shape normative expectations of behavior.[19] Views like this have emerged in government policies. For example, Britain's National Cyber Strategy of 2020 posits that its "approach to cyber deterrence does not yet seem to have fundamentally altered the risk calculus for attackers."[20]

Another challenge stems from the inherent difficulties in defense and deterrence that render countermeasures an inadequate form of response. In other words, had defense and deterrence been adequate, countermeasures would not be needed. This argument has some merits; after all, the addition of countermeasures to defenders' toolkit is likely to broaden the mission to the extent that it becomes hard to keep the aim "limited." The concern with mission creep can be mitigated, however, when actors declare intent on countering in advance and if they launch countermeasures clearly and demonstrably for defensive purposes. When states make clear their conditions for launching countermeasures, they simultaneously reduce the chance of escalation.

2. Defending critical infrastructure and its challenges

Countermeasures are appropriate when deployed to defend critical infrastructure from cyber-attacks. In the face of the recent rise of ransomware attacks and public attention on the need to defend critical infrastructure, the public is more readily accepting of countermeasures.

As resources are limited, decision makers must prioritize which sectors of the network to defend. However, as of June 2022, while there are many national guidelines and policies on critical infrastructure, there are no global guidelines on what critical infrastructure is and how we can digitally protect it, which then allows states to operate with various sets of definitions.[21] When the US identifies a set of 16 sectors, Russia's "critically important objects" are six, with 48 different sub-sectors.[22] There are countries without a definition, including China. Beijing refers to critical information infrastructure (CII) as systems that, "if destroyed, suffering a loss of function, or experiencing leakage of data might seriously endanger national security, national welfare, the people's livelihood, or the public interest," but there are no components given as examples.[23] This means that every conceivable item can be considered an illegitimate target in China's cyberspace, so any cyber-attack on China could be interpreted as one on CII, a ground for retaliation. That is why, for instance, RAND researchers fear that "cyber activity on the power grid that fits well within one country's definition of espionage could be interpreted by another country as an imminent attack."[24]

The problem is that hackers may not be on the same page as to what states consider critical infrastructure. They may not have a clear idea of what critical infrastructure includes and what is considered an illegitimate target. Besides, if critical infrastructure crosses so many properties at once, how are hackers supposed to know what to avoid *and* how to avoid them in their operations? Are there any targets that can be "legitimate"? The questions are critical because there is no communication between hackers and states about what they mean "legitimate" targeting is, if any. This lack of mutual understanding allows hackers to invoke plausible deniability and unilaterally expect victims to take no preventive action, another recipe for disaster.

Not surprisingly, this problem is not limited to critical infrastructure; research points to similar problems in supply-chains sectors. A study of government policy in Britain, the US, and the European Union on chemical, energy, and water sectors unearthed a variety of interpretations for "supply chain," which resulted in different quantities and qualities of advice offered by authorities and sectors. The absence of a common language has generated challenges to support supply chain procurement, risk management, and limited coverage.[25] Solutions to these challenges are hard to come by, in part because they need to come not from individual states but from the international community at large. While the international community would need to determine what sectors would be protected and ensure that hackers know it, achieving this is difficult as sectors that would be excluded from the category would certainly oppose this effort. Debate would take years to complete, if at all, requiring stakeholders to determine which sector would be considered as critical infrastructure. To coordinate in the prototypical "two-level negotiation" is extremely hard, especially because countries have conflicting priorities and different amounts of resources to spend on it.

3. Compliance with rules of behavior

Finally, countermeasures are legitimate when they conform to a host of behavioral norms. This condition has been debated for over a decade in venues like the United Nations (UN) Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG). Making sure that cyberspace activities comply with existing global rules ensures the legitimacy of its operations. Another reason why we need explicit signs of international compliance is that some states would otherwise consider countermeasures excessively provocative. They may find it so controversial to carry out countermeasures that they require international approval before going ahead with them. Countries like Japan, for instance, have tried to move forward to strengthen their defenses through cross-domain concepts, but Japan has found it quite difficult to carry out active defense because of its unique constitutional, social, and political environments.[26] National debate has proceeded to where officials have refrained from officially developing cyberweapons for defense. Thus, for countries to move forward with the agenda of countermeasures, they must first make efforts to craft a strategic framework in which countermeasures would gain public legitimacy through voluntary compliance with rules of behavior.

The importance of adherence to cyberspace norms has been widely recognized in cybersecurity literature. Strategic cyber scholars have stressed the role of ethical integrity as a key enabler of norm diffusion,[27] but they also emphasize the social benefits of operational restraint.[28] Furthermore, they stress the need for us to understand how international rules encourage actors to comply with norms of cyberspace behavior and to merge humanitarian values with technical expertise.[29] The call for synergy has prompted the participation of major technology firms like Microsoft in the discourse around setting norms and increased the number of advocates for a ban on attacks on critical infrastructure.[30] For example, Robert Collett stresses communication and consultation to generate an actionable framework, prioritize national capacity needs, and give compelling narrative to consolidate the outcome.[31]

Under the principles of necessity and distinction, respectively, states would launch countermeasures only when they faced grave and imminent peril and would do so in ways that avoid causing excessive harm or hitting civilians and units used by noncombatants for nonmilitary purposes (for instance, hospitals). Under the principle of proportionality, states would not launch countermeasures in ways that would be excessive relative to the strike against them. Under the principle of due diligence, states should be proactive so that their territory is not used for operations that produce adverse consequences for other states.

Even though each of these principles works differently, they remain mutually beneficial. That is, the more principles are respected by the international community, the more likely they are to have collective effects against illicit actions. Furthermore, the more states complying with each of the principles, the more likely the international community is to have stronger legitimacy in using the principles to discourage malicious operations. Yet the interlocking

relationship of the principles and actors presumes that there must be a critical mass of countries that abide by the principles. The challenge is that there is a limited number of states able and willing to comply with the principles.

At the same time, policymakers must acknowledge that these principles will not be a perfect shield against malicious actions. Research shows that they are especially ineffective against OCO by non-state actors.[32] Partly because of these problems, the norms and principles stated above have repeatedly been ignored. Hackers have collaborated with China, Russia, North Korea, Britain, and the US to spy on each other to help them reinforce their great power ambitions.[33] The GGE and OEWG are gathering to address a range of enforceable conditions under which violators of the laws and norms would be penalized.

CONCLUSION

In this article, I discussed some of the most important strategic aspects of conducting countermeasures as part of offensive cyber. Countermeasures can be justified as an appropriate mode of offensive cyber under the assumptions of the limited aim of defense and deterrence, protection of critical infrastructure, and compliance with rules of behavior. At the same time, there are challenges with carrying them out as a form of offensive cyber. First is that there are various degrees of feasibility about what conditions can be met for countermeasures to be appropriate. Second, there are challenges with meeting each of the conditions themselves. The challenges are hard to solve, which may explain why it has been so hard for the international community to yield a set of agreeable criteria for active defense measures. It is also important to note that strategic effectiveness and legality may not necessarily equal ethical maturity of options even if they are conducted for purely defensive or deterrent purposes, because they involve intrusive actions that can be seen as "offensive." This suggests that there may be other conditions we may have to examine.

All this leads to a somewhat pessimistic assessment of countermeasures as part of offensive cyber. There is no excuse, however, for the international community to not develop more defensive and deterrent options. The aim of this paper was to describe opportunities for active defense options, spell out relevant challenges with the process of carrying out the measures, and generate a host of solutions to deal with them. More work need to be done, especially in terms of finding out what other components of countermeasures need to be put into a comprehensive framework of offensive cyber to make them a legitimate means of active defense.

NOTES

1. The US Department of Defense, *Cyber Operations, Joint Publication* 3-12 (June 8, 2018).
2. Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Rowman & Littlefield: Lanham, MD, 2017), 18-9.
3. Dorothy Denning and Bradley Strawser, "Active Cyber Defense: Applying Air Defense to the Cyber Domain," in *Understanding Cyber Conflict: 14 Analogies,* eds. George Perkovich and Ariel Levite (Washington, DC: Georgetown University Press, 2017), 194.
4. Fifth Domain, "Here's how Cyber Command is using 'defend forward'" (November 12, 2019).
5. Michael Fischerkeller and Richard Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," *Cyber Defense Review*, Special Edition (2019), 276-77.
6. See NATO, "Allied Joint Publication-3.20 Allied Joint Doctrine for Cyberspace Operations" (January 2020), 22.
7. See, for instance, Chon Abraham and Sally Daultrey, "Considerations for NATO in Reconciling Challenges to Shared Cyber Threat Intelligence: A study of Japan, the US and the UK," NATO CCDCOE, eds., *Cyber Threats and NATO 2030: Horizon Scanning and Analysis* (Tallinn, Estonia, 2021).
8. It is possible that the recent development of the trilateral security pact between Australia, the United Kingdom, and the United States (AUKUS) may bring Australia even closer to the ties between Britain and the United States. On the other hand, US allies like Japan may be tempted to be part of growing collaboration among these countries, especially through the ongoing Quad cooperation mechanism (Australia, Japan, India, and the United States), although as of June 2022, Japan's case is restricted to its bilateral alliance with the United States. The Guardian, "Japan should work with Aukus on cybersecurity and AI, says Shinzo Abe" (November 19, 2021).
9. Jeppe Jacobsen, "Cyber offense in NATO: challenges and opportunities," *International Affairs,* Vol. 97, No. 3 (May 2021), abstract.
10. James Pattison, "From defense to offence: The ethics of private cybersecurity," *European Journal of International Security,* Vol. 5, No. 2 (2020), 233-34.
11. Michael Chertoff, *Exploding Data: Reclaiming Our Cyber Security in the Digital Age* (New York: Grove Press, 2018), 188-91.
12. Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge: Cambridge University Press, 2020), 113-200.
13. Cyberscoop, "A 'lot' of firms are developing offensive cyber techniques, hoping for investment" (October 18, 2021).
14. Lawrence Cavaiola, David Gompert, and Martin Libicki, "Cyber House Rules: On War, Retaliation and Escalation," *Survival,* Vol. 57, No. 1 (2015); Jason Healey, "The Cartwright Conjecture: The Deterrent Value and Escalatory Risks of Fearsome Cyber Capabilities," in Lin and Zegart, eds., *Bytes, Bombs, and Spies.*
15. Perri Adams, Dave Aitel, George Perkovich, and JD Work, "Responsible Cyber Offense," *Lawfare* (August 2, 2021).
16. Cyberscoop, "Nations investing in cyber, 'democratization' of malware are factors accelerating dangers online, CISA official says" (October 18, 2021).
17. Paul Ducheine and Peter Pijpers, "The Missing Component in Deterrence Theory: The Legal Framework," in Frans Osinga and Tim Sweijs, eds., *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century – Insights from Theory and Practice* (The Hague: T.M.C. Asser Press, 2021), 487.
18. Joseph Brown and Tanisha Fazal, "#SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations," *European Journal of International Security,* Vol. 6, No. 4 (2021).
19. Michael Fischerkeller and Richard Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," *Orbis,* Vol. 61, No. 3 (2017), 382.
20. The Cabinet Office of the United Kingdom, *National Cyber Strategy* (2022), 25.
21. Cecilia Gallais and Eric Filiol, "Critical Infrastructure: Where Do We Stand Today? A Comprehensive and Comparative Study of the Definitions of a Critical Infrastructure, "*Journal of Information Warfare,* Vol. 16, No. 1 (Winter 2017), 64-65.
22. Christer Pursiainen, "Russia's Critical Infrastructure Policy: What do we Know About it?" *European Journal for Security Research*, Vol. 6 (2021), 25.
23. Graham Webster, Samm Sacks, and Paul Triolo, "Three Chinese Digital Economy Policies at Stake in the U.S.-China Talks," *New America* (April 2, 2019).

NOTES

24. Anu Narayanan, et al., *Deterring Attacks Against the Power Grid: Two Approaches for the U.S. Department of Defense* (Santa Monica, CA: RAND Corporation, 2020), pp., xv-xvi. Also see Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations* (Oxford: Oxford University Press, 2016), Chapter 4.
25. Colin Topping, Andrew Dwyer, Ola Michalec, Barnaby Craggs, and Awais Rashid, "Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks," *Computers & Security,* Vol. 108 (September 2021).
26. Nori Katagiri, "From Cyber Denial to Cyber Punishment: What Keeps Japanese Warriors from Active Defense Operations?" *Asian Security*, Vol. 17, No. 3 (2021).
27. Martha Finnemore and Duncan Hollis, "Constructing Norms for Global Cybersecurity," American Journal of International Law, Vol. 110 (2019).
28. Joseph Nye, "Deterrence and Dissuasion in Cyberspace," *International Security*, Vol. 41, No. 3 (Winter 2016/17), 60.
29. *Matthias Kettemann, The Normative Order of the Internet: A Theory of Rule and Regulation Online* (Oxford: Oxford University Press, 2020).
30. Louise Marie Hurel and Luisa Cruz Lobato, "Unpacking cyber norms: private companies as norm entrepreneurs," *Journal of Cyber Policy*, Vol. 3, No. 1 (2018).
31. Robert Collett, "Understanding cybersecurity capacity building and its relationship to norms and confidence building measures," *Journal of Cyber Policy* (2021).
32. Nori Katagiri, "Why International Law and Norms Do Little in Preventing Non-State Cyber Attacks," *Journal of Cybersecurity,* Vol. 7, No. 1 (2021).
33. Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020).